DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LOS PROCESOS DE GESTIÓN DE INFORMACIÓN, GESTIÓN DE RECURSOS FÍSICOS Y GESTIÓN HUMANA DE LA EMPRESA ACCESO DIRECTO ASOCIADOS LIMITADA, BASADO EN LA NORMA ISO 27001:2013

KAREN LIZETH GIRALDO VALENCIA
KAREN VIVIANA VILLALOBOS ROJAS

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2017

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LOS PROCESOS DE GESTIÓN DE INFORMACIÓN, GESTIÓN DE RECURSOS FÍSICOS Y GESTIÓN HUMANA DE LA EMPRESA ACCESO DIRECTO ASOCIADOS LIMITADA, BASADO EN LA NORMA ISO 27001:2013.

KAREN LIZETH GIRALDO VALENCIA
KAREN VIVIANA VILLALOBOS ROJAS

Tesis de Grado para optar por el título de Especialista en Seguridad Informática

Asesora
Lorena Ocampo Correa
Ingeniera De Sistemas

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2017

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá, viernes 03 de marzo de 2017.

DEDICATORIA

Dedico esta tesis en primer lugar a Dios por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor. A mi padre Jaime Villalobos y a mi esposo Diego Suescún quienes fueron un gran apoyo emocional durante el tiempo en que escribía esta tesis. A mi amiga Karen Giraldo quien me apoyo y alentó para continuar, cuando parecía que me iba a rendir y a mi hermano Jaime Andrés que nunca dudo para ayudarme y apoyarme en todo momento. Gracias por tu tiempo, tus consejos, apoyo incondicional y por tu cariño.

Para ellos es esta dedicatoria de tesis, pues es a ellos a quienes se las debo por su apoyo incondicional.

KAREN VIVIANA VILLALOBOS ROJAS

Primero a Dios por su amor infinito, por haberme dado la vida, la fortaleza y la fe necesaria para dar un paso más en mi desarrollo profesional, a mi madre Gloria Valencia quien ha estado conmigo durante todo este proceso, quien con su esfuerzo y apoyo me impulso a seguir adelante en los momentos de dificultad, mi heroína quien supo trasmitirme su mayor riqueza a través de la mejor lección de vida que puede recibir un ser humano “El ejemplo”. A mi amiga Karen Villalobos quien ha recorrido este camino conmigo, mi compañera en esta aventura llamada proyecto de grado. A todas y cada una de las personas que tuvieron una palabra de apoyo en el momento indicado y a la Universidad Piloto de Colombia por una lección más de vida.

KAREN LIZETH GIRALDO VALENCIA

AGRADECIMIENTOS

En primer lugar, gracias infinitas a Dios el dador de todas las cosas quien ha guiado nuestro camino por el sendero correcto y quien nos permite llegar a este punto dando un paso más en nuestro proyecto de vida.

Agradecimientos especiales a **ACCESO DIRECTO,** especialmente a la señora **Luz Marina Gamarra Barrios** gerente de la empresa por su confianza y colaboración al abrir las puertas de su empresa y disponer de su personal para que este proyecto se llevara a cabo.

Una mención de gratitud al ingeniero **Oscar Javier Lemus Hurtado** encargado de la oficina de sistemas por su tiempo y profesionalismo al momento de compartir información específica de la oficina y los procesos principales involucrados en el proyecto.

Por la orientación, la ayuda y paciencia un agradecimiento sincero a la ingeniera **Lorena Ocampo Correa** quien al compartir sus conocimientos nos permitió afianzar mucho más de lo aprendido en el proceso de la especialización.

Agradecemos a la Universidad Piloto de Colombia y a todos los docentes involucrados en nuestro proceso de aprendizaje, por su dedicación, orientación y guía que fueron fundamentales para nosotras.

CONTENIDO

LISTA DE GRÁFICAS

pág.

LISTA DE CUADROS

pág.

GLOSARIO DE TÉRMINOS

AMENAZA: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.[1]

AUDITORÍA: proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.[2]

CONTROL: las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. También se utiliza como sinónimo de salvaguarda o contramedida.[3]

DESASTRE: cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.[4]

DISPONIBILIDAD: acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.[5]

EVALUACIÓN DE RIESGOS: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.[6]

GESTIÓN DE RIESGOS: proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.[7]

IMPACTO: el coste para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros pérdida de reputación, implicaciones legales, etc.[8]

---

[1] SISTEMA DE GESTIÓN DE SEGURIDAD LA INFORMACIÓN, ISO27001. (27 de Febrero de 2017). Obtenido de SISTEMA DE GESTIÓN DE SEGURIDAD LA INFORMACIÓN, ISO27001: http://www.ceeisec.com/nuevaweb/doc/FORMACION_SGSI_2 010.pdf
[2] Ibíd,.
[3] Ibíd,.
[4] Ibíd,.
[5] Ibíd,.
[6] Ibíd,.
[7] Ibíd,.
[8] Ibíd,.

INTEGRIDAD: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.[9]

INVENTARIO DE ACTIVOS: lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.[10]

ISO 27001: estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable.[11]

RIESGO: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.[12]

RIESGO RESIDUAL: el riesgo que permanece tras el tratamiento del riesgo inesperado o no deseado que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.[13]

SEGURIDAD DE LA INFORMACIÓN: preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.[14]

SGSI: la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)[15]

---

[9] Ibíd,.
[10] Ibíd,.
[11] Ibíd,.
[12] Ibíd,.
[13] Ibíd,.
[14] Ibíd,.
[15] Ibíd,.

INTRODUCCIÓN

La era tecnológica, la expansión de las redes y la interoperabilidad entre las diferentes tecnologías hacen que día a día los sistemas de información se encuentren expuestos a vulnerabilidades o amenazas que pueden llegar a poner en riesgo activos de información. Por ser la información uno de los activos más importantes de toda organización, la seguridad de la misma se ha convertido en un tema estratégico organizacional, ya sea por cultura propia o por regulaciones legales que así lo establecen.

Estadísticas publicadas por compañías especializadas en seguridad de la información, muestran que un gran porcentaje de las amenazas informáticas provienen del interior de las organizaciones, situación que en buena medida se debe a la resistencia al cambio y el incumplimiento de las políticas por parte del personal de la misma.

Para mitigar los riesgos de acceso no autorizado, divulgación o pérdida de información, las organizaciones deben adoptar todas las medidas de seguridad que estén a su alcance para gestionar apropiadamente los riesgos. Un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2013 es un mecanismo eficaz para gestionar las amenazas y vulnerabilidades que puedan afectar los activos de información de las organizaciones.

1. PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

En pleno siglo XXI para nadie es un secreto que en casi todas las empresas independientemente del tipo de empresa que sea, entre el 85% y 95% de la información se maneja de forma digital, con la era de la digitalización no solamente ha llegado la rapidez y mejora en algunos de los procesos, sino también las vulnerabilidades y problemas con respecto a la seguridad de la información, pero, la pregunta más importante radica en: ¿Cómo corre más peligro nuestra información? Cuando una persona con un alto nivel de conocimiento informático intenta acceder a ella desde afuera, o cuando los mismos funcionarios internos no toman las precauciones y el manejo adecuado con la información, especialmente en este caso que hablamos de información confidencial.

La empresa Acceso Directo Asociados Limitada, a pesar que cuenta con recursos tecnológicos, presenta problemas entre los que se destaca la inexistencia de procesos como gestión de la información, gestión de los recursos físicos, gestión humana, gestión de políticas de seguridad, manejo de inventarios, control de equipos audiovisuales y de cómputo, no cuentan con un mapa de análisis de riesgos y controles de los mismos, no cuenta con un sistema de gestión de incidentes de seguridad de la información, Acceso Directo Asociados Limitada no cuenta con un Sistema de Gestión de Seguridad, el cual permite que la empresa preste un servicio o producto de manera confiable y de conformidad con las especificaciones internacionales.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo podría Acceso Directo Asociados Limitada proteger de forma apropiada sus objetivos e ideales de negocio para asegurar la explotación de nuevas oportunidades en el mercado actual?

2. JUSTIFICACIÓN

El diseño de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2013, suministrará los medios necesarios para la gobernabilidad, oportunidad y viabilidad a fin de que la seguridad de la información apoye y amplíe los objetivos estratégicos de la empresa, mediante la protección de su información la cual es fundamental para garantizar la debida gestión financiera, administrativa y operativa de la empresa.

La implementación y mantenimiento de un SGSI (Sistema de Gestión de Seguridad de la Información), muestra el compromiso de la organización con la seguridad de la información y proporciona los elementos necesarios para gestionar de manera adecuada los riesgos que puedan afectar la seguridad de su información, lo cual genera confianza en sus clientes que es primordial para el crecimiento y la sostenibilidad de la empresa.

Este proyecto busca diseñar un SGSI para los procesos de gestión de información, gestión de recursos físicos y gestión humana en la empresa Acceso Directo Asociados Limitada, puesto que de esta manera la calidad del servicio en cuanto al manejo de información crítica se va a ver ampliamente mejorado, es claro que la empresa tiene una necesidad inmediata de gestionar y mitigar las amenazas y vulnerabilidades que puedan afectar de manera parcial o total su sistema de información, con la elaboración del mapa de riesgos se da el primer paso para llevar a cabo el proceso en mención, además de esto, ayudará a crear y desarrollar cultura de seguridad en todo el personal de la organización.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un sistema de gestión de seguridad de la información para los procesos de gestión de información, gestión de recursos físicos y gestión humana para la empresa Acceso Directo Asociados Limitada bajo la norma ISO 27001:2013.

3.2 OBJETIVOS ESPECÍFICOS

- Describir el estado actual de la empresa Acceso Directo Asociados Limitada, en cuanto a la seguridad de la información por medio de un análisis de brecha (GAP).

- Realizar el levantamiento de activos de la empresa Acceso Directo Asociados Limitada.

- Analizar los riesgos de la información según los requerimientos de la norma ISO 27001:2013.

- Definir los controles y planes de tratamiento de riesgos de seguridad de la información con base en la norma ISO 27001:2013.

- Definir la política del sistema de gestión de seguridad de la información bajo por la norma ISO 27001:2013 de acuerdo con los resultados del proceso de gestión de riesgos.

4. ALCANCE

Este proyecto tiene como objetivo diseñar un Sistema de Gestión de la Seguridad de la Información bajo el estándar ISO 27001:2013 para la empresa Acceso Directo Asociados Limitada, la cual ofrece el servicio de estrategias de divulgación (diseñan campañas de publicidad y/o comunicaciones internas y externas que visibilizan la imagen, producto y servicio) del cliente los cuales son del sector público. Cabe destacar que la prestación del servicio de estrategias de divulgación es el inicio del sistema de gestión, donde las etapas posteriores son la implementación de controles, auditorías externas e internas, temas legales entre otras tareas, así como el proceso de gestión que será llevado a cabo por la gerencia, por lo cual la decisión de su implementación, seguimiento y mejora continua es responsabilidad de la organización.

5. MARCO REFERENCIAL

5.1 MARCO TEÓRICO

A continuación, se presenta el marco teórico del presente proyecto.

5.1.1 Sistema de gestión de seguridad de la información. El sistema de gestión de seguridad de la información es el concepto central sobre el que se construye ISO 27001, la gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. (ISO 27000.es, 2016)

Para garantizar que el sistema de gestión de seguridad de la información sea gestionado de forma correcta se tiene que identificar el ciclo de vida y los aspectos relevantes adoptados para garantizar:

- **Confidencialidad:** La información no se pone a disposición de nadie, ni se revela a individuos o entidades no autorizadas.
- **Integridad:** Mantener de forma completa y exacta la información y los métodos de proceso.
- **Disponibilidad:** Acceder y utilizar la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades autorizadas cuando lo requieran.

Según el conocimiento que se tiene del ciclo de vida de la información relevante se puede adoptar la utilización de un proceso sistemático, documentado y conocido por toda la empresa desde un enfoque de riesgos empresarial.

La información, junto a los procesos y los sistemas que hacen uso de ella, son activos demasiado importantes para la empresa. La confidencialidad, integridad y disponibilidad de dicha información puede ser esencial para mantener los niveles de competitividad, conformidad, rentabilidad e imagen de la empresa necesarios para conseguir los objetivos de la misma y asegurar así que haya beneficios económicos.

Las empresas y los sistemas de información se encuentran expuestos a un número cada vez más elevado de amenazas aprovechando así cualquier tipo de vulnerabilidad para someter a los activos críticos de información a ataques, espionajes, vandalismo, etc. Los virus informáticos o los ataques son ejemplos muy comunes y conocidos, pero también se deben asumir los riesgos de sufrir incidentes de seguridad que pueden ser causados voluntariamente o involuntariamente desde dentro de la propia empresa o los que son provocados de forma accidental por catástrofes naturales.

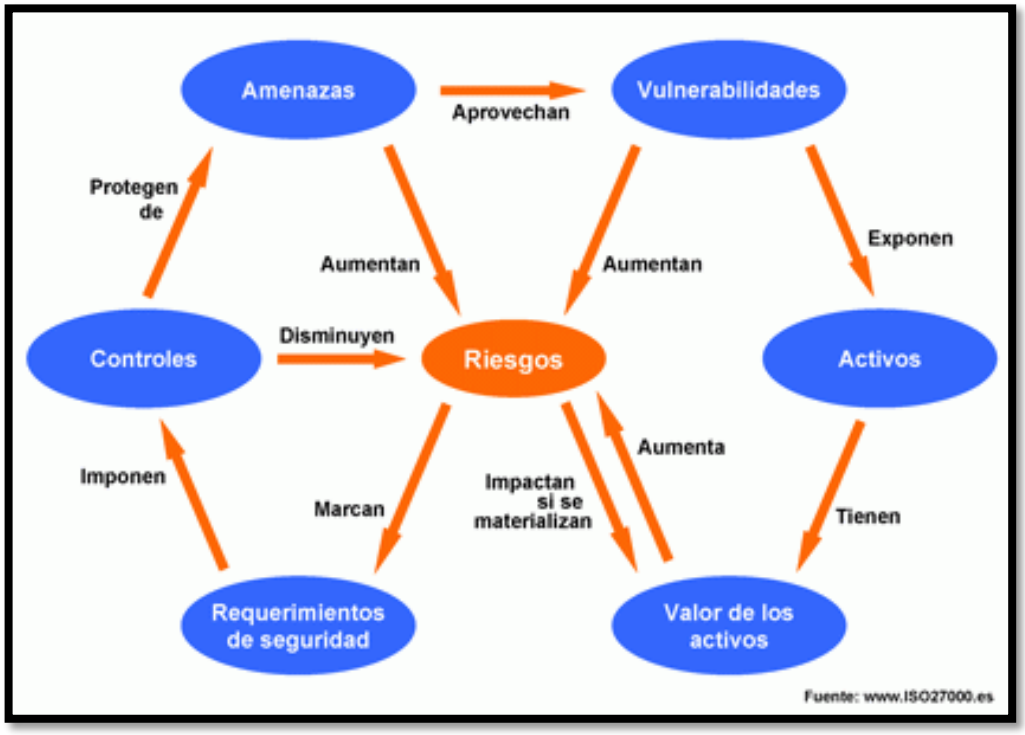
El cumplimiento de la legislación, la adaptación dinámica y de forma puntual de todas las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar que se obtenga el máximo beneficio, son algunos de los aspectos fundamentales en los que un SGSI sirve como herramienta de gran utilidad y de importante ayuda para la gestión de las empresas.

El nivel de seguridad que se alcanza gracias a los medios técnicos es limitado e insuficiente por sí mismo, durante la gestión efectiva de la seguridad debe tomar parte activa toda la empresa, con la gerencia al frente, tomando en consideración a los clientes y a los proveedores de la organización.

El modelo de gestión de la seguridad tiene que contemplar unos procedimientos adecuados y planificar e implementar controles de seguridad que se basan en una evaluación de riesgos y en una medición de la eficiencia de los mismos.

Para entender que es el SGSI, se debe tener en cuenta que este ayuda a establecer la política de seguridad y los procedimientos en relación a los objetivos del negocio, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir. Ver Gráfica 1. Utilidad de un SGSI.

Gráfica 1. Utilidad de un SGSI



Fuente: (ISO 27000.es, 2016)[16]

5.1.1.2 Beneficios. Los beneficios de implementar el SGSI son:

- Establecer una metodología de gestión de la seguridad estructurada y clara.
- Reducir el riesgo de pérdida, robo o corrupción de la información sensible.
- Los clientes tienen acceso a la información mediante medidas de seguridad.
- Los riesgos y los controles son continuamente revisados.
- Se garantiza la confianza de los clientes y los socios de la organización.

[16] EL PORTAL DE ISO 27001 EN ESPAÑOL, ISO 27000. [Online]. [Consultado el 16 de marzo de 2016]. Disponible en: http://www.iso27000.es/sgsi.html

- Las auditorías externas ayudan de forma cíclica a identificar las debilidades del SGSI y las áreas que se deben mejorar.
- Facilita la integración con otros sistemas de gestión.
- Se garantiza la continuidad de negocio tras un incidente grave.
- Cumple con la legislación vigente sobre información personal, propiedad intelectual y otras.
- La imagen de la organización a nivel internacional mejora.
- Aumenta la confianza y las reglas claras para las personas de la empresa.
- Reduce los costos y la mejora de los procesos y el servicio.
- Se incrementa la motivación y la satisfacción del personal.
- Aumenta la seguridad en base la gestión de procesos en lugar de una compra sistemática de productos y tecnologías.

5.1.1.3 Documentación. La documentación mínima que se debe tener en cuenta a la hora de implementar un SGSI es:

- Política y objetivos de seguridad.
- El alcance del SGSI.
- Los procedimientos y los controles que apoyan al SGSI.
- Describir toda la metodología a la hora de realizar una evaluación de riesgo.
- Generar un informe después de realizar la evaluación de riesgo.
- Realizar un plan de tratamiento de riesgos.
- Procedimientos de planificación, manejo y control de los procesos de seguridad de la información y de medición de la eficacia de los controles.

- Declaración de aplicabilidad.
- Procedimiento de gestión de toda la documentación del SGSI. (SGSI Blog especializado en Sistemas de Gestión , 2016).

- **Sistema de Gestión de Seguridad de la Información**: Según el estándar internacional ISO 27001 el submodelo de procesos define de forma sistémica el camino que se debe seguir para realizar un proyecto de análisis y gestión de riesgos. Este submodelo es el marco de trabajo en el que se agrupan y ordenan todas las acciones que se realizan, además incluye todas las dificultades para conseguirlo, resumiendo define lo siguiente:

  Estructurar el proyecto sirve de guía al equipo de trabajo y permite involucrar en él a los responsables de activos que hay que proteger y a los clientes.

  El submodelo de procesos es capaz de formalizar las diferentes acciones, las sucesiones y la estructura en tres niveles diferentes: etapas, actividades y tareas.

  En cada etapa se agrupan diferentes actividades, establece los hitos de decisión y consigue los productos intermedios y finales. En cada actividad se agrupan las diferentes tareas con criterios de carácter funcional. En cada terea se describe el trabajo realizado en el mínimo componente del desglose y suele asignarse a un solo tipo de puesto y de ejecutantes.

- **Que incluye un Sistema de Gestión de Seguridad de la Información:** La documentación de un sistema de gestión de seguridad de la información se ha mostrado siempre como una pirámide de 4 niveles, los cuales se constituyen así:

  Documentos de Nivel 1. Manual de seguridad: Por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. Este sería el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.

  Documentos de Nivel 2. Procedimientos: Documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

Documentos de Nivel 3. **Instrucciones, checklists y formularios:** Documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

Documentos de Nivel 4. Registros: Documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos. De manera específica, ISO 27001 indica que un SGSI debe estar formado por los siguientes documentos (en cualquier formato o tipo de medio):

- **Alcance del SGSI:** Ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).

- **Política y objetivos de seguridad:** Documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.

- **Enfoque de evaluación de riesgos:** Descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables.

- **Informe de evaluación de riesgos:** Estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.

- **Plan de tratamiento de riesgos:** Documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.

- **Procedimientos documentados:** Todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.

- **Registros:** Documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.

Control de la documentación: Para los documentos generados se debe establecer, documentar, implantar y mantener un procedimiento que defina las acciones de gestión necesarias para:

- Aprobar documentos apropiados antes de su emisión.
- Revisar y actualizar documentos cuando sea necesario y renovar su validez.
- Garantizar que los cambios y el estado actual de revisión de los documentos están identificados.
- Garantizar que los documentos se mantienen legibles y fácilmente identificables.
- Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente destruidos acorde con los procedimientos aplicables según su clasificación.
- Garantizar que los documentos procedentes del exterior están identificados.
- Garantizar que la distribución de documentos está controlada.
- Prevenir la utilización de documentos obsoletos.
- Aplicar la identificación apropiada a documentos que son retenidos con algún propósito.

(Sistema de Gestión de la Seguridad de la información, 2017)

5.2 MARCO NORMATIVO

A continuación, se presenta el marco normativo a tener en cuenta:

5.2.1 Norma ISO 27001:2013. Esta norma ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de seguridad de la información (SGSI). La adopción de un SGSI debería ser una decisión estratégica para una organización. El diseño e implementación de un SGSI de una organización están influenciados para las necesidades, objetivos, los requisitos de seguridad, los procesos empleados, el tamaño y estructura de la organización.

Esta norma promueve la adopción de un enfoque basado en procesos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el SGSI de una organización para funcionar eficazmente.

La norma ISO 27001:2013 cubre todo tipo de organizaciones por ejemplo empresas comerciales, agencias gubernamentales, organizaciones sin ánimo de lucro. Esta norma específica los requisitos para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos globales del negocio de la organización, especifica los requisitos para la implementación de controles de seguridad adaptados a las necesidades de las organizaciones individuales o a parte de ellas.

El SGSI está diseñado para asegurar controles de seguridad suficientes y proporcionales que protejan los activos de la información y brinden confianza a las partes interesas[17].

5.2.2 ISO 27001 2013 pasos a seguir en una evaluación de riesgos. ISO 27001 2013 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una organización, abordando las personas, los procesos y la tecnología. La revisión más reciente de esta norma fue publicada en 2013, como bien acompaña a su nombre, pero no se debe olvidar que la primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

---

[17] ICONTEC. (2009). COMPENDIO SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). Bogotá: ICONTEC.

La norma ISO 27001 2013 puede ser implementada en cualquier tipo de organización o empresa, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en la materia, proporcionando una metodología para implementar correctamente la gestión de la seguridad de la información en una empresa. También permite que una organización sea certificada, pero debe llevarse a cabo por un organismo de certificación independiente, pues la Organización Internacional de Normalización no emite certificados. Dicha certificación confirmará que la seguridad de la información ha sido implementada en esa empresa bajo el cumplimiento de la norma ISO 27001 2013.

Recientemente, el Instituto Nacional de Estándares y Tecnología, conocido como NIST por sus siglas en inglés, ha citado a la norma ISO 27001:2013 como una norma de gran importancia dentro de su marco nacional de ciberseguridad, lo que les otorga aún más relevancia a las empresas con intereses en EE.UU. y las empresas estadounidenses responsables de la protección crítica de la infraestructura.

El despliegue de la norma ISO 27001:2013 requiere una empresa para llevar a cabo las evaluaciones de riesgos de seguridad de la información. Esto es para asegurar que los controles de seguridad de la información que se están implementando son apropiadas para el tipo de información que está siendo almacenada, procesada o transmitida.

El enfoque actual de los pasos a seguir para llevar a cabo la evaluación de riesgos de seguridad de la información incluye:

- Establecer un marco de evaluación de riesgos: El marco se encarga de definir cuestiones como la capacidad de riesgo y la cultura de la empresa, las escalas de riesgo que se van a utilizar, así como la metodología a seguir a la hora de evaluar riesgos de seguridad de la información.

- Identificar los riesgos: Posiblemente es la parte más difícil y la que mayor tiempo del proceso consume. Puede encontrarse más fácilmente tras una evaluación del riesgo basada en activos, de tal modo que se identifiquen todos y cada uno de los riesgos que pueden afectar a los activos de información. También resulta de gran utilidad el libre acceso a una biblioteca o registro de riesgos y amenazas que puedan afectar a la organización.

- Analizar y evaluar los riesgos: El análisis y la evaluación de los riesgos conllevan un proceso de asignación de valores concretos para determinar la probabilidad y el impacto en la empresa de los distintos riesgos, y para definir cómo encajan estos en el umbral de aceptación del riesgo. Se debe ser capaz de concretar cuáles de los riesgos son prioridades que requieren medidas urgentes y cuáles tienen un nivel de prioridad medio o aceptable.

- Seleccione las opciones de gestión del riesgo: Cuando se hayan determinado los riesgos, se debe establecer si se desean gestionar, admitir, eliminar o transferir. Para gestionar los riesgos se debe hacer uso de los controles de seguridad de la información adecuados. Es de gran utilidad tener acceso a los controles establecidos bajo la norma ISO 27001 2013, sobre todo basándonos en las políticas fijadas según la norma e incorporadas previamente a cada uno de los controles.

- Revisión, informe y mantenimiento: Una cuestión de gran importancia respecto a la realización de la evaluación de riesgos para el cumplimiento de la norma ISO 27001 es naturalmente, el posterior desarrollo del conjunto de informes donde se recogen cuáles son los riesgos, las medidas que se van a llevar a cabo para gestionarlos, cada uno de los plazos para la implementación de los controles y las distintas acciones accesorias. Respecto a esto, aparecen en la norma ISO 27001:2013 dos documentos de relevancia, como son la Declaración de Aplicabilidad (SOA) y el plan de gestión de riesgos[18].

[18] ISO 27001 2013: Pasos a seguir en una evaluación de riesgos. (19 de Febrero de 2017). Obtenido de SGSI Blog especializado en Sistemas de Gestión : http://www.pmg-ssi.com/2016/05/iso-27001-2013-pasos-seguir-evaluacion-riesgos/

6. DISEÑO METODOLÓGICO

A continuación, se presenta el diseño metodológico establecido para el presente proyecto.

6.1 HISTORIA DE LA EMPRESA

Acceso Directo Asociados Limitada, es una empresa dedicada a ofrecer servicios de Estrategias de Divulgación (Diseñar campañas de publicidad y/o comunicaciones internas y externas que visibilizan la imagen, producto y servicio) del cliente.

“La perseverancia, el deseo de prestar un servicio con calidad y la búsqueda por hacer de su capital humano el más competitivo han sido el soporte institucional.

Con el tiempo el área de comunicaciones fue fortaleciéndose hasta quedar convertida en agencia de comunicaciones y publicidad. Mientras el área de tecnología consolidó algunos de sus servicios de apoyo técnico empresarial en sistemas se convirtió en pieza fundamental para el desarrollo del servicio de comunicación digital y cómo área de soporte técnico para toda la empresa.

De los cuatro socios iniciales, son dos quienes hoy lideran la empresa que con 15 años de vida empresarial ha tenido un crecimiento racional y sin pausa, soportando algunos de sus procesos en proveedores aliados y generando cerca de 60 empleos indirectos y 10 directos.

Lo anterior le permite atender comercialmente a entidades del Estado, empresas multinacionales, gremios y otras empresas del sector privado, haciéndoles sentir que son su único cliente, porque en Acceso Directo Asociados Limitada todos los clientes son importantes, pues se constituyen en su razón de ser.”

Misión: Somos una empresa consultora que ofrece productos y servicios de comunicación, publicidad y tecnología, implementa en todos sus procesos el mejoramiento continuo para la satisfacción de las necesidades de nuestros clientes internos y externos.

Visión: Ser en el 2018 una empresa consultora de productos y servicios de comunicación, publicidad y tecnología cuya cobertura en Bogotá represente el 80% del total de las ventas, 15% en otras ciudades del país y 5% en otros países de Latinoamérica. [19]

Objetivos de negocio: Uno de los objetivos de negocio de la empresa Acceso Directo Asociados Limitada, es aportar soluciones de valor agregado a los clientes de la empresa para que crezca la reputación tanto en marcas, como rentabilidad y cifras de negocio.

Incrementar la reputación corporativa de los clientes de la empresa, se traza un plan a cada cliente con el fin de mejorar la reputación corporativa a percepción de los clientes finales, el plan incluye detección de errores y potenciación de ventajas en cada campaña realizada.

Objetivos específicos de negocio:

1. Elaboración de campañas publicitarias creando nuevas ideas y diseños, para una mejora continua y lograr así un buen posicionamiento dentro del mercado.

2. Vender la imagen corporativa en distintos medios publicitarios, ofreciendo calidad y responsabilidad en cada una de las campañas a realizar.

Ideales de Negocio:

Entre los ideales de negocio de la empresa Acceso Directo Asociados Limitada, se encuentran:

1. Lograr renombre en el mercado, potenciando las marcas de sus clientes y comunicar con éxito sus campañas publicitarias.

2. Principio de transparencia en el manejo de las comunicaciones de los clientes.

3. Confidencialidad, de tal forma que la gestión en comunicaciones, relacionados con publicidad, promoción y relaciones públicas de los clientes se maneja de

[19] ACCESO DIRECTO. (28 de Noviembre de 2016). Obtenido de ACCESO DIRECTO: http://accesodirecto.com.co/web/es

manera absolutamente reservada y se fundamente en la integridad de la estrategia.

4. Honestidad, con las ofertas que se presenten, con el servicio que se entregue, con la información que se transmita.

5. Lealtad, para con los clientes.

Oportunidades actuales de negocio en el mercado: Actualmente la empresa Acceso Directo Asociados Limitada, maneja en su gran mayoría campañas publicitarias con empresas estatales o públicas, conseguidas por medio de licitaciones públicas, por acuerdos de confidencialidad las razones sociales de las empresas no pueden ser publicadas en este documento, sin embargo, se puede especificar que las campañas más importantes son con empresas públicas a nivel local, municipal, departamental y algunas campañas son con empresas estatales a nivel nacional, estas campañas publicitarias corresponden al 80% del total de proyectos de la empresa Acceso Directo Asociados Limitada, el otro 20% es un mercado poco explorado por la empresa que corresponden a entidades privadas, actualmente, solo se hacen campañas publicitarias con pequeñas empresas privadas, que no alcanzan un nivel de relevancia significativo.

6.2 DIAGNÓSTICO

A continuación, se analizará el estado actual de seguridad de la información de Acceso Directo Asociados Limitada.

La situación actual de la empresa con respecto al área de seguridad de la información, la pone en desventaja con respecto a su competencia directa en el mercado, puesto que las campañas publicitarias, especialmente las relacionadas con clientes potenciales se ven muy expuestas al plagio, al manejar niveles casi nulos de confidencialidad.

6.2.1 Análisis GAP basado en los controles de la norma ISO 27001:2013. El análisis de brecha o análisis GAP se realiza como parte de la identificación del estado actual del cumplimiento de Acceso Directo Asociados Limitada, en cuanto a la seguridad de la información, el análisis GAP se realizó con respecto a los requisitos y controles descritos en el anexo A de la norma ISO 27001:2013,

mediante el uso de la herramienta GAP o análisis de brecha se determina el estado actual y el estado al que se quiere llegar.

A partir del análisis que se realice posterior a la obtención de los resultados, se dará a conocer el estado actual de la empresa respecto al cumplimento de los requisitos y controles definidos por la norma ISO27001:2013 para el diseño de un sistema de gestión de seguridad de la información y las acciones y recursos que serán requeridos para lograr el cumplimiento del estado al que se desea llegar partiendo del estado en el que se encuentra actualmente la empresa.

6.2.1.1 Objetivo. Realizar una revisión para determinar el estado actual del cumplimiento respecto a los requisitos y los controles del anexo A definidos por la norma ISO 27001:2013.

6.2.1.2 Alcance de la revisión. La revisión se llevará a cabo teniendo en cuenta los requisitos y controles descritos en el anexo A de la norma ISO 27001:2013.

6.2.1.3 Metodología y evidencia de la revisión. Para llevar a cabo la revisión se hizo uso de una lista de verificación basada en los requerimientos de la norma ISO 27001:2013 incluyendo el anexo A de la misma, el cuestionario que se formuló a manera de entrevista, se aplicó al ingeniero Oscar Javier Lemus Hurtado encargado de la oficina de sistemas de la empresa Acceso Directo Asociados Limitada, que en el momento es la persona que mayor conocimiento tiene del tema.

El cuestionario se compone de 5 campos, los cuales incluyen, criterio según la norma ISO 27001:2013 el cual hace relación al numeral descrito en la norma, el campo descripción donde se encuentra la pregunta que fue formulada al ingeniero de la oficina de sistemas, un campo de comentarios, donde se encuentran descritas las respuestas dadas a los interrogantes, campo observaciones/hallazgos donde el auditor tiene espacio para hacer las observaciones que considere necesarias, porcentaje de implementación, es una calificación dada en porcentajes del 0 al 100% en relación a la situación real de la empresa Acceso Directo Asociados Limitada.

A partir del resultado obtenido de la revisión descrita en el anexo A, se evidencian los resultados en 2 secciones, la primera hace referencia al anexo A de la norma ISO 27001:2013 y la segunda a los resultados obtenidos del cumplimiento de los numerales del 4 al 10 de la norma ISO 27001:2013.

Cuadro 1. Análisis GAP

							CÓDIGO: GF-110 VERSIÓN: 1	
				LISTA DE VERIFICACIÓN PARA AUDITORÍAS INTERNAS ISO 27001:2013				
Vigencia del Programa:	Desde							
Ciclo No.								
Fecha Auditoría	Desde	6	11	2016	9	11	2016	
Fecha Elaboración:		9	11	2016				
Proceso:								
Objetivo Auditoría:	Realizar una revisión para determinar el estado actual de cumplimientos respecto a los requisitos y los controles del anexo A definidos por la norma ISO 27001:2013.							
Alcance Auditoría:	Revisar controles de la ISO 27001:2013							
Auditor Líder:	Karen Viviana Villalobos Rojas				Karen Lizeth Giraldo Valencia			
Nombre Auditado:	Acceso Directo Asociados Limitada							
CREACIÓN LISTA DE VERIFICACIÓN								
Criterio ISO 27001:2013	**Descripción**	**Comentarios para el Auditor y saber que temas debe tener en cuenta para preguntar o para el Auditado y preparar la auditoría**			**Observaciones/ Hallazgos**		**% Implementación**	
4	**CONTEXTO DE LA ORGANIZACIÓN**							
4.1 CONOCIMIENTO DE LA ORGANIZACIÓN Y SU CONTEXTO:	¿La organización determina las cuestiones internas y externas que son pertinentes para la finalidad de SGSI?	Se tienen identificados los factores internos y externos, pero no se cuenta con ningún tipo de documentación			N/A		20%	
4.2. COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS	¿Cómo determinan las partes interesadas y sus requisitos que son pertinentes al sistema de gestión de la seguridad de la información?	Los requisitos de las partes interesadas pueden incluir los requisitos legales y reglamentarios, y las obligaciones contractuales.			N/A		20%	

Cuadro 1. (Continuación)

Criterio ISO 27001:2013	Descripción	Comentarios para el Auditor y saber que temas debe tener en cuenta para preguntar o para el Auditado y preparar la auditoría	Observaciones/ Hallazgos	% Implementación
4.3. DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	¿Cómo determinan los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance?	Tener en cuenta las cuestiones externas e internas referidas en el numeral 4.1, los requisitos referidos en el numeral 4.2; para los procesos definidos. El alcance debe estar disponible como información documentada	Los limites y la aplicabilidad del sistema de gestión de la seguridad de la información serán definidas en el diseño que se entregue	0%
4.4. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	¿Cómo se establece, implementa, mantiene y mejora continuamente el sistema de gestión de la seguridad de la información?	Se cumple si a su vez se cumplen los requisitos de norma, se debe formalizar su establecimiento e implementación de acuerdo a los procesos que tenga definidos la empresa, además evidenciar que se mantiene y mejora de acuerdo a como la empresa defina sus procesos de los sistemas de gestión.	No existe la implementación, mantenimiento y mejora continua del SGSI ya que no existe.	0%
5	**LIDERAZGO**			
5.1. LIDERAZGO Y COMPROMISO	¿Se tiene una política de la seguridad de la información y los objetivos de la seguridad de la información?	No existe	N/A	0%
	¿Se ha identificado como la seguridad de la información se integra con los objetivos del negocio y procesos de la organización?	No se ha identificado	N/A	0%
	¿La empresa dispone de recursos destinados al sistema de seguridad de la información?	Se ha dispuesto de una persona como apoyo al proceso (jefe de la oficina de sistemas) Se dispone de la información total sobre los 3 procesos en los cuales se basa el diseño del SGSI	N/A	60%
	¿Se ha informado a la organización de la necesidad y los beneficios de un sistema de gestión de seguridad de la información?	Se dio una capacitación a la gerencia de la empresa sobre la importancia de un SGSI, posterior al entendimiento de este, se procede a firmar el acuerdo de confidencialidad	N/A	60%
	¿Se promueve la mejora continua del SGSI?	Como la empresa no cuenta con un SGSI, este numeral no aplica	N/A	0%

Cuadro 1. (Continuación)

Criterio ISO 27001:2013	Descripción	Comentarios para el Auditor y saber que temas debe tener en cuenta para preguntar o para el Auditado y preparar la auditoría	Observaciones/ Hallazgos	% Implementación
5.2. POLÍTICA	¿La empresa cuenta con una política de seguridad de la información que incluya objetivos relacionados con la seguridad de la información y el compromiso de mejora continua?	No existe política de seguridad de la información	N/A	0%
5.3. ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN	¿Se han definido roles y responsabilidades respecto a la seguridad de la información?	No se cuentan con roles definidos para seguridad de la información, todos los procesos relacionados con TI se manejan en la oficina de sistemas	N/A	0%
6	**PLANIFICACIÓN**			
6.1. ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES	¿Cómo se planifican las acciones para tratar los riesgos y oportunidades?	No hay una matriz de riesgos para identificación de riesgos	N/A	0%
	¿Se cuenta con un proceso de valoración de riesgos de la seguridad de la información?	No se cuenta con este proceso	N/A	0%
	¿Se identifican los riesgos de seguridad de la Información?	No	N/A	0%
	¿Está definido y documentado el proceso de tratamiento de riesgos de seguridad de la información?	No está definido	N/A	0%
	¿Están determinados todos los controles que son necesarios para implementar las opciones escogidas para el tratamiento de riesgos de seguridad de la información?	No existen controles	N/A	0%
6.2 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y PLANES PARA LOGRARLO	¿Están establecidos los objetivos de seguridad de la información?	Evidenciarlo en el documento que haya definido la entidad para este propósito	Queda pendiente por parte de nosotros la definición de los Objetivos de Seguridad de la Información.	0%

Cuadro 1. (Continuación)

Criterio ISO 27001:2013	Descripción	Comentarios para el Auditor y saber que temas debe tener en cuenta para preguntar o para el Auditado y preparar la auditoría	Observaciones/ Hallazgos	% Implementación
7	**SOPORTE**			
7.1 RECURSOS	¿Se han determinado y proporcionados los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información?	No se han determinado recursos	N/A	0%
7.2 COMPETENCIA	¿Se conoce el nivel de competencia o conocimiento de los funcionarios de la empresa respecto a la seguridad dela información?	Todos los funcionarios de la entidad hacen una prueba de manejo de tecnologías de la información entre sus pruebas de ingreso	N/A	20%
7.3. TOMA DE CONCIENCIA	¿Los funcionarios de la empresa conocen las políticas, objetivos y los beneficios del sistema de gestión de seguridad de la información?	No	N/A	0%
7.4 COMUNICACIÓN	¿Se ha comunicado a los miembros de la organización o terceros las políticas, objetivos y los beneficios del sistema de gestión de seguridad de la información?	No	N/A	0%
7.5 INFORMACIÓN DOCUMENTADA	¿Se encuentran documentadas las políticas, objetivos e información general del sistema de gestión de seguridad de la información?	No	N/A	0%
8	**OPERACIÓN**			
8.1. PLANIFICACIÓN Y CONTROL OPERACIONAL	¿Se han definido actividades basadas en un sistema de mejora continua que permita cumplir los objetivos, políticas y requisitos de la seguridad de la información?	No	N/A	0%
8.2. VALORACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	¿Se llevan a cabo valoraciones de riesgo de la seguridad de la información?	No	N/A	0%

Cuadro 1. (Continuación)

Criterio ISO 27001:2013	Descripción	Comentarios para el Auditor y saber que temas debe tener en cuenta para preguntar o para el Auditado y preparar la auditoría	Observaciones/ Hallazgos	% Implementación
8.3. TRATAMIENTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN	¿Se han generado planes de tratamiento de los riesgos?	No se han generado	N/A	0%
9	**EVALUACIÓN DEL DESEMPEÑO**			
9.1. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN	¿Se mide de alguna manera el desempeño del sistema de gestión de seguridad de la información?	No	N/A	0%
9.2 AUDITORÍA INTERNA	¿Están planificados y establecidos los programas de auditorías internas?	No	N/A	0%
9.3 REVISIÓN POR LA DIRECCIÓN	¿La alta dirección revisa los resultados del proceso de auditoría y medición del desempeño del sistema de gestión de seguridad de la información?	No	N/A	0%
10	**MEJORA**			
10.1 NO CONFORMIDADES Y ACCIONES CORRECTIVAS	¿Están documentadas las no conformidades, las acciones tomadas y los resultados de las acciones correctivas?	No	N/A	0%
10.2 MEJORA CONTINUA	¿Se evidencia la mejora de la convivencia, adecuación, y eficacia del sistema de gestión de seguridad de la Información?	No	Por ahora no se realiza.	0%

Cuadro 1. (Continuación)

Criterio ISO 27001:2013	Descripción	Comentarios para el Auditor y saber que temas debe tener en cuenta para preguntar o para el Auditado y preparar la auditoría	Observaciones/ Hallazgos	% Implementación
ANEXO A				
5	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**			
5.1	**DIRECTRICES ESTABLECIDAS POR LA DIRECCIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN**			
5.1.1 POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN:	¿Se evidencia la existencia de políticas, para la seguridad de la información, que hayan sido aprobadas, publicadas, y comunicadas a los empleados?	No	N/A	0%
5.1.2 REVISIÓN DE LAS POLÍTICAS PARA SEGURIDAD DE LA INFORMACIÓN	¿La organización revisa, las políticas de seguridad de la información?	No	N/A	0%
6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**			
6.1	**ORGANIZACIÓN INTERNA**			
6.1.1 ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN	¿De qué manera se evidencia la asignación de responsabilidades en seguridad de la información?	No se evidencia esta asignación porque el área no está definida	No están definidos roles de seguridad	0%
6.1.2 SEPARACIÓN DE DEBERES	¿La organización garantiza que los deberes y responsabilidades respecto al área de seguridad de la información?	No se evidencia esta asignación porque el área no está definida	N/A	0%
6.1.3 CONTACTO CON LAS AUTORIDADES	¿Se tiene algún contacto con autoridades o entidades que requieran la aplicación de estándares de seguridad de la información?	No existe contacto con ninguna autoridad de seguridad de la información	N/A	0%
6.1.4 CONTACTO CON GRUPOS DE INTERÉS SOCIAL	¿La empresa tiene contacto con grupos de interés o foros especializados en seguridad de la información?	No	N/A	0%

Cuadro 1. (Continuación)

Criterio ISO 27001:2013	Descripción	Comentarios para el Auditor y saber que temas debe tener en cuenta para preguntar o para el Auditado y preparar la auditoría	Observaciones/ Hallazgos	% Implementación
6.1.5 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LOS PROYECTOS	¿Se aplica la seguridad de la información en la gestión de proyectos?	No	N/A	0%
6.2	**DISPOSITIVOS MÓVILES Y TELETRABAJO**			
6.2.1 POLÍTICA PARA DISPOSITIVOS MÓVILES	¿Cuál es la política de seguridad para el uso de dispositivos móviles?	No existe	No se cuenta con una política	0%
6.2.2 TELETRABAJO	¿Cuál es la política de seguridad para el teletrabajo?	No hay política sobre teletrabajo	N/A	0%
7	**SEGURIDAD DE LOS RECURSOS HUMANOS**			
7.1	**ANTES DE ASUMIR EL EMPLEO**			
7.1.1 ROLES Y RESPONSABILIDADES	¿Cómo realiza la verificación de antecedentes de los candidatos a un empleo?	Se hacen pruebas dependiendo el rol que se va a realizar. Pruebas de técnicas Pruebas Psicotécnicas	Si se realiza la revisión de antecedentes disciplinarios	60%
7.1.2 TÉRMINOS Y CONDICIONES DE EMPLEO	¿De qué manera definen las responsabilidades en seguridad como parte del contrato de vinculación a la organización?	Validar la existencia de acuerdos de confidencialidad y no divulgación, y código de conducta.	Cláusulas de confidencialidad: Si existe	80%

Cuadro 1. (Continuación)

Criterio ISO 27001:2013	Descripción	Comentarios para el Auditor y saber que temas debe tener en cuenta para preguntar o para el Auditado y preparar la auditoría	Observaciones/ Hallazgos	% Implementación
7.2	**DURANTE LA EJECUCIÓN DEL EMPLEO**			
7.2.1 RESPONSABILIDADES DE LA DIRECCIÓN	¿La organización exige a sus empleados y contratistas el cumplimiento de las políticas de seguridad definidas?	No	No están definidas	0%
7.2.2 TOMA DE CONCIENCIA, EDUCACIÓN Y FORMACIÓN EN LA SEGURIDAD DE LA INFORMACIÓN	¿Se incluye la formación y concienciación de la seguridad de la información a empleados y contratistas en intervalos específicos?	No	N/A	0%
7.2.3 PROCESO DISCIPLINARIO	¿Existe el proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad?	No	N/A	0%
7.3	**TERMINACIÓN O CAMBIO DE EMPLEO**			
7.3.1 TERMINACIÓN O CAMBIO DE RESPONSABILIDADES DE EMPLEO	¿La empresa comunica y hace cumplir las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de contrato?	No	No, porque no hay un SGSI, ni políticas definidas	0%
8	**GESTIÓN DE ACTIVOS**			
8.1	**RESPONSABILIDAD POR LOS ACTIVOS**			
8.1.1 INVENTARIO DE ACTIVOS	¿Se han identificado los activos de información que permiten el cumplimiento de los objetivos del negocio?	Existe un inventario de los equipos de cómputo, audiovisuales y de los activos de información que pertenecen a la empresa	N/A	60%
8.1.2 PROPIEDAD DE LOS ACTIVOS	¿En el inventario de activos se mantienen únicamente aquellos que son propiedad de la organización?	La empresa solo cuenta con equipos propios, no existen activos de terceros	N/A	40%
	¿La organización, cómo clasifica los activos?	Los inventarios están clasificados por área	No se cuenta con una metodología de clasificación	
8.1.3 USO ACEPTABLE DE LOS ACTIVOS	¿Se han definido políticas en las cuales se establecen los usos aceptables de los activos?	No	N/A	0%

Cuadro 1. (Continuación)

Criterio ISO 27001:2013	Descripción	Comentarios para el Auditor y saber que temas debe tener en cuenta para preguntar o para el Auditado y preparar la auditoría	Observaciones/ Hallazgos	% Implementación
8.1.4 DEVOLUCIÓN DE LOS ACTIVOS	¿Aquellos activos que son propiedad de la organización deben ser retornados por los empleados/contratistas al finalizar la relación laboral?	Si	N/A	80%
8.2	**CLASIFICACIÓN DE LA INFORMACIÓN**			
8.2.1 CLASIFICACIÓN DE LA INFORMACIÓN	¿Se ha clasificado la información de acuerdo a los principios de confidencialidad, integridad y disponibilidad y su importancia para el negocio?	No	N/A	0%
8.2.2 ETIQUETADO DE LA INFORMACIÓN	¿Se ha definido un proceso para identificar la información de acuerdo a la clasificación dada?	No	N/A	0%
8.2.3 MANEJO DE ACTIVOS	¿Se ha definido un proceso para la administración de activos de acuerdo con la clasificación dada?	No	N/A	0%
8.3	**MANEJO DE MEDIOS**			
8.3.1 GESTIÓN DE MEDIOS REMOVIBLES	¿Se ha definido una política para controlar el uso de medios removibles?	No	N/A	0%
8.3.2 DISPOSICIÓN DE LOS MEDIOS	¿Existen procedimientos para disponer en forma segura de los medios cuando ya no se requieran?	No	N/A	0%
8.3.3 TRANSFERENCIA DE MEDIOS FÍSICOS	¿Se garantiza que los medios que contienen información se protegen contra acceso no autorizado, uso indebido o corrupción durante el transporte?	No	N/A	0%
	¿Se realiza el registro que identifique el contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte, y el recibo en su destino?	No	N/A	

Cuadro 1. (Continuación)

Criterio ISO 27001:2013	Descripción	Comentarios para el Auditor y saber que temas debe tener en cuenta para preguntar o para el Auditado y preparar la auditoría	Observaciones/ Hallazgos	% Implementación
9	**CONTROL DE ACCESO**			
9.1	**REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO**			
9.1.1 POLÍTICA DE CONTROL DE ACCESO	¿Se ha definido una política de control de acceso de acuerdo a los objetivos del negocio y de seguridad de la información?	No	N/A	0%
	¿Está definida la separación de roles de control de acceso?	No están definidas	N/A	
9.1.2 ACCESO A REDES Y A SERVICIOS EN RED	¿Se garantiza que solo se permita acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente?	No	N/A	0%
9.2	**GESTIÓN DE ACCESO DE USUARIOS**			
9.2.1 REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS	¿Se tiene implementado una política/procedimiento para la creación/eliminación de cuentas de usuario?	No	N/A	0%
9.2.2 SUMINISTRO DE ACCESO DE USUARIOS	¿Se tiene implementado un proceso para asignar/retirar derechos de usuario?	No	N/A	0%
9.2.3 GESTIÓN DE DERECHOS DE ACCESO PRIVILEGIADO	¿Se controla la asignación y uso de derechos de acceso privilegiado?	No	N/A	0%
9.2.4 GESTIÓN DE INFORMACIÓN DE AUTENTICACIÓN SECRETA DE USUARIOS	¿Se tiene implementado un proceso para autenticación secreta?	No	N/A	0%
9.2.5 REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIOS	¿Se revisa la asignación de derechos de usuario en intervalos específicos?	No	N/A	0%
9.2.6 RETIRO O AJUSTE DE LOS DERECHOS DE ACCESO	¿La asignación de derechos de usuario debe cancelarse cuando el funcionario finaliza la relación laboral con la compañía?	No	N/A	0%

Cuadro 1. (Continuación)

Criterio ISO 27001:2013	Descripción	Comentarios para el Auditor y saber que temas debe tener en cuenta para preguntar o para el Auditado y preparar la auditoría	Observaciones/ Hallazgos	% Implementación
9.3	**RESPONSABILIDADES DE LOS USUARIOS**			
9.3.1 USO DE INFORMACIÓN DE AUTENTICACIÓN SECRETA	¿Se exige a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta?	No	No se encuentra definida esta política	0%
	¿Existen lineamientos definidos en la empresa para la generación de contraseñas seguras?	No	N/A	
9.4	**CONTROL DE ACCESO A SISTEMAS Y APLICACIONES**			
9.4.1 RESTRICCIÓN DE ACCESO A LA INFORMACIÓN	¿Existe política de control de acceso?	No	No hay	0%
	¿Se ha definido una política para restringir el acceso a aplicaciones basado en funciones o responsabilidades?	No, los funcionarios pueden asumir cualquier rol de acuerdo a las necesidades de la organización	N/A	
9.4.2 PROCEDIMIENTO DE INGRESO SEGURO	¿Cuál es el procedimiento de ingreso seguro a sistemas y aplicaciones?	No está definido	N/A	0%
9.4.3 SISTEMA DE GESTIÓN DE CONTRASEÑAS	¿Se tiene definida una política de contraseñas que asegure la calidad de estas?	No	N/A	0%
9.4.4 USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS	¿Se tiene una política que restrinja el uso de software que puedan anular o sobrepasar las políticas de seguridad o control de acceso?	No	Se tiene proceso, pero no está documentado	40%
9.4.5 CONTROL DE ACCESO A CÓDIGOS FUENTE DE PROGRAMAS	¿Se restringe el acceso a los códigos fuente de los programas?	No se tiene una política definida para esto	N/A	0%

Cuadro 1. (Continuación)

Criterio ISO 27001:2013	Descripción	Comentarios para el Auditor y saber que temas debe tener en cuenta para preguntar o para el Auditado y preparar la auditoría	Observaciones/ Hallazgos	% Implementación
10	**CRIPTOGRAFÍA**			
10.1	**CONTROLES CRIPTOGRÁFICOS**			
10.1.1 POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS	¿Se tiene una política sobre el uso de controles criptográficos para proteger la información que se almacena o intercambia?	No	No está definida	0%
10.1.2 GESTIÓN DE LLAVES	¿Existe una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida?	No	No se tiene información cifrada	0%
11	**SEGURIDAD FÍSICA Y DEL ENTORNO**			
11.1	**ÁREAS SEGURAS**			
11.1.1 PERÍMETRO DE SEGURIDAD FÍSICA	¿Se han definido áreas en las que se implementen controles de seguridad para proteger información confidencial??	No existen áreas restringidas	Las oficinas más importantes cuentan con puertas con llave	40%
11.1.2 CONTROLES FÍSICOS DE ENTRADA	¿Se implementan controles para garantizar que solo se permita el ingreso de personal autorizado??	Si	Control en portería del edificio	40%
	¿De qué manera lleva el registro de entrada y salida de visitantes?	Libro de registro de entrada y salida	N/A	
	¿Existen mecanismos de autenticación están implementados para las áreas que almacén información confidencial?	No	N/A	
11.1.3 SEGURIDAD DE OFICINAS, RECINTOS E INSTALACIONES	¿Se ha diseñado seguridad física a las instalaciones de compañía??	CCTV, Guarda de seguridad	N/A	60%

Cuadro 1. (Continuación)

Criterio ISO 27001:2013	Descripción	Comentarios para el Auditor y saber que temas debe tener en cuenta para preguntar o para el Auditado y preparar la auditoría	Observaciones/ Hallazgos	% Implementación
11.1.4 PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES	¿Se han contemplado medidas de seguridad frente a amenazas de tipo natural o accidentes?	No	N/A	0%
11.1.5 TRABAJO EN ÁREAS SEGURAS	¿Se aplican controles para trabajo en áreas seguras?	No	N/A	0%
11.1.6 ÁREAS DE DESPACHO Y CARGA	¿Están definidas áreas de despacho y de carga?	No aplica	N/A	0%
11.2	**EQUIPOS**			
11.2.1 UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS	¿Se implementan medidas para proteger los equipos de amenazas del entorno y limitar el uso no autorizado?	No	No se tiene una política definida de creación de usuarios y contraseñas, los portátiles que tiene la empresa no cuentan con guayas (algunos)	20%
11.2.2 SERVICIOS DE SUMINISTRO	¿Cómo se protegen los equipos contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro?	No hay sistemas definidos	N/A	0%
11.2.3 SEGURIDAD DEL CABLEADO	¿Se han implementado medidas para proteger el cableado eléctrico, de red y de telecomunicaciones?	En la parte externa la protección que brinda el operador de internet, en la parte interna la caja de paso de propiedad del edificio	N/A	40%
11.2.4 MANTENIMIENTO DE EQUIPOS	¿Existe un plan de mantenimiento de equipos para asegurar su disponibilidad e integridad continuas?	No	Solo se le hace mantenimiento a los equipos cuando estos fallan	20%

Cuadro 1. (Continuación)

Criterio ISO 27001:2013	Descripción	Comentarios para el Auditor y saber que temas debe tener en cuenta para preguntar o para el Auditado y preparar la auditoría	Observaciones/ Hallazgos	% Implementación
11.2.5 RETIRO DE ACTIVOS	¿Se controla que los equipos, información o software no se retiren de su sitio sin autorización previa?	No	N/A	0%
11.2.6 SEGURIDAD DE EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES	¿Existen medidas de seguridad para los activos que se encuentran fuera de las instalaciones de la organización, se tienen implementadas?	No	No se cuenta con controles	0%
11.2.7 DISPOSICIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS	¿Se aplican procedimientos para el borrado seguro de información en medios de almacenamiento, discos duros o software que serán reusados o puestos fuera de funcionamiento?	No	No se cuenta con política de borrado seguro	0%
11.2.8 EQUIPOS DE USUARIO DESATENDIDOS	¿Se asegura que a los equipos desatendidos se les dé protección apropiada?	No	No se puede asegurar el uso de equipos desatendidos porque no cuentan con contraseñas	0%
11.2.9 POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA	¿Se tiene definida una política de escritorio limpio para los papeles y medios de almacenamiento removibles?	No	N/A	0%
12	**SEGURIDAD DE LAS OPERACIONES**			
12.1	**PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES**			
12.1.1 PROCEDIMIENTOS DE OPERACIÓN DOCUMENTADOS	¿Los procedimientos de encendido y apagado, copias de respaldo, mantenimiento de equipos, manejo de medios, manejo de correo, entre otros donde se encuentran documentados y publicados?	No	No se tienen documentados, tampoco están publicados, pero se aplican algunos mediante la comunicación verbal	60%
12.1.2 GESTIÓN DE CAMBIOS	¿Se controlan los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información?	Si	El área de sistemas no cuenta con sistema de gestión de cambios, las demás áreas si	40%
12.1.3 GESTIÓN DE CAPACIDAD	¿Se hace seguimiento al uso de los recursos y se planifica la capacidad para asegurar el funcionamiento del sistema??	No	N/A	0%

Cuadro 1. (Continuación)

Criterio ISO 27001:2013	Descripción	Comentarios para el Auditor y saber que temas debe tener en cuenta para preguntar o para el Auditado y preparar la auditoría	Observaciones/ Hallazgos	% Implementación
12.1.4 SEPARACIÓN DE LOS AMBIENTES DE DESARROLLO, PRUEBAS Y OPERACIÓN	¿Cuáles son los ambientes separados de desarrollo, prueba y operación?	No aplica	La empresa no realiza ningún tipo de desarrollo	0%
12.2	**PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS**			
12.3	**COPIAS DE RESPALDO**			
12.3.1 RESPALDO DE LA INFORMACIÓN	¿Cómo se hacen las copias de respaldo de la información, del software e imágenes de los sistemas?	Se saca un *Backup* periódicamente (cada 15 días) en discos duros externos	N/A	40%
12.4	**REGISTRO Y SEGUIMIENTO**			
12.4.1 REGISTRO DE EVENTOS	¿Se elaboran, conservan y revisan regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información?	No	N/A	0%
12.4.2 PROTECCIÓN DE LA INFORMACIÓN DE REGISTRO	¿Se protegen los registros frente acceso no autorizado y manipulación??	No	N/A	0%
12.4.3 REGISTROS DEL ADMINISTRADOR Y DEL OPERADOR	¿Se registran, protegen y revisan con regularidad las actividades del administrador y del operador del sistema?	No se llevan a cabo estas actividades	N/A	0%
12.4.4 SINCRONIZACIÓN DE RELOJES	¿Se tiene definida una política de sincronización de tiempo y se sincronizan los relojes de los sistemas con una fuente valida?	No, cada equipo maneja la hora local	N/A	0%

Cuadro 1. (Continuación)

Criterio ISO 27001:2013	Descripción	Comentarios para el Auditor y saber que temas debe tener en cuenta para preguntar o para el Auditado y preparar la auditoría	Observaciones/ Hallazgos	% Implementación
12.5	**CONTROL DE SOFTWARE OPERACIONAL**			
12.5.1 INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS	¿Se tienen definidos procedimientos para la instalación de sistemas operativos?	Se tiene un procedimiento desde la oficina de sistemas, aunque no se encuentra documentado	Solo la persona de la oficina de sistemas está autorizada para hacerlo	20%
12.6	**GESTIÓN DE LA VULNERABILIDAD TÉCNICA**			
12.6.1 GESTIÓN DE VULNERABILIDADES TÉCNICAS	¿Se tiene definida una política y se realizan pruebas de vulnerabilidad para determinar el grado de exposición a estas?	No	N/A	0%
12.6.2 RESTRICCIONES SOBRE LA INSTALACIÓN DE SOFTWARE	¿Existen controles para la instalación de software por parte de los usuarios?	Si	La política no se encuentra documentada	20%
12.7	**CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN**			
12.7.1 CONTROLES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN	¿Se planifican y realizan auditorías sobre los sistemas operativos teniendo en cuenta la continuidad del negocio?	No	N/A	0%
13	**SEGURIDAD DE LAS COMUNICACIONES**			
13.1	**GESTIÓN DE LA SEGURIDAD DE LAS REDES**			
13.1.1 CONTROLES DE REDES	¿Se tienen definidos políticas y controles para gestionar, controlar y proteger la seguridad de la información en sistemas y aplicaciones?	No	N/A	0%
13.1.2 SEGURIDAD DE LOS SERVICIOS DE RED	¿Se identifican los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red?	No se lleva a cabo esta identificación	Cuentan con ANS con los proveedores de servicio.	20%

Cuadro 1. (Continuación)

Criterio ISO 27001:2013	Descripción	Comentarios para el Auditor y saber que temas debe tener en cuenta para preguntar o para el Auditado y preparar la auditoría	Observaciones/ Hallazgos	% Implementación
13.1.3 SEPARACIÓN EN LAS REDES	¿Los sistemas de información, usuarios y servicios se encuentran separadas?	No	N/A	0%
13.2	**TRANSFERENCIA DE INFORMACIÓN**			
13.2.1 POLÍTICAS Y PROCEDIMIENTOS DE TRANSFERENCIA DE INFORMACIÓN	¿Se tienen definidos políticas y controles para asegurar la seguridad de la información que se transmite por la red?	La información se intercambia con clientes a través de correo electrónico, lo que se trabaja en cliente se queda en el cliente, el cliente define sus políticas de respaldo	N/A	0%
13.2.2 ACUERDOS SOBRE TRANSFERENCIA DE INFORMACIÓN	¿Existen acuerdos establecidos para la transferencia segura de información del negocio entre la organización y las partes externas?	Existen, pero no está documentado, hasta el momento se hace de forma verbal	N/A	20%
13.2.3 MENSAJERÍA ELECTRÓNICA	¿Se protege la información que es intercambiada mediante mensajes electrónicos?	No	N/A	0%
13.2.4 ACUERDOS DE CONFIDENCIALIDAD O DE NO DIVULGACIÓN	¿Se tienen identificados los requisitos de confidencialidad y no divulgación de información que reflejan las necesidades de protección de la información?	No	No se encuentran definidos como tal, ya que no hay documentación de los mismo y los acuerdos verbales son poco confiables	20%

Cuadro 1. (Continuación)

Criterio ISO 27001:2013	Descripción	Comentarios para el Auditor y saber que temas debe tener en cuenta para preguntar o para el Auditado y preparar la auditoría	Observaciones/ Hallazgos	% Implementación
14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**			
14.1	**REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN**			
14.1.1 ANÁLISIS Y ESPECIFICACIÓN DE REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN	¿Se definen los requisitos relacionados con seguridad de la información que se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes?	No	N/A	0%
14.1.2 SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS	¿Para aplicaciones usadas a través de redes públicas se aplican controles para mitigar actividades fraudulentas, disputas contractuales, divulgación y modificación no autorizadas?	No se aplican controles	N/A	0%
14.1.3 PROTECCIÓN DE TRANSACCIONES DE LOS SERVICIOS DE LAS APLICACIONES	¿Se protege la información involucrada en las transacciones de los servicios de las aplicaciones para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada?	No existen sistemas de protección	N/A	0%
14.2	**SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE**			
14.2.1 POLÍTICA DE DESARROLLO SEGURO	¿Se contemplan aspectos de seguridad que se están contemplando en la Política de Desarrollo Seguro?	No Aplica	La empresa no realiza ningún tipo de desarrollo	No Aplica
14.2.2 PROCEDIMIENTOS DE CONTROL DE CAMBIOS EN SISTEMAS	¿Cuáles son los procedimientos formales de control de cambios a los sistemas dentro del ciclo de vida de desarrollo?	No Aplica	La empresa no realiza ningún tipo de desarrollo	No Aplica

Cuadro 1. (Continuación)

Criterio ISO 27001:2013	Descripción	Comentarios para el Auditor y saber que temas debe tener en cuenta para preguntar o para el Auditado y preparar la auditoría	Observaciones/ Hallazgos	% Implementación
14.2.3 REVISIÓN TÉCNICA DE LAS APLICACIONES DESPUÉS DE CAMBIOS EN LA PLATAFORMA DE OPERACIÓN	¿Se realizan revisiones a aplicaciones propias o centradas por clientes?	No Aplica	La empresa no realiza ningún tipo de desarrollo	No Aplica
14.2.4 RESTRICCIONES EN LOS CAMBIOS A LOS PAQUETES DE SOFTWARE	¿Se controlan las modificaciones a los paquetes de software?	No Aplica	La empresa no realiza ningún tipo de desarrollo	No Aplica
14.2.5 PRINCIPIOS DE CONSTRUCCIÓN DE SISTEMAS SEGUROS	¿Se documentan los principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información?	No Aplica	La empresa no realiza ningún tipo de desarrollo	No Aplica
14.2.6 AMBIENTE DE DESARROLLO SEGURO	¿Se establecen y protegen adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas?	No Aplica	La empresa no realiza ningún tipo de desarrollo	No Aplica
14.2.7 DESARROLLO CONTRATADO EXTERNAMENTE	¿Se supervisa y hace seguimiento a las actividades de desarrollo de sistemas contratados externamente?	No Aplica	Se utiliza software comercial, con códigos fuente ya compilados	No Aplica
14.2.8 PRUEBAS DE SEGURIDAD DE SISTEMAS	¿Se hacen pruebas de funcionalidad de la seguridad se llevan a cabo en el desarrollo?	No Aplica	N/A	No Aplica

Cuadro 1. (Continuación)

Criterio ISO 27001:2013	Descripción	Comentarios para el Auditor y saber que temas debe tener en cuenta para preguntar o para el Auditado y preparar la auditoría	Observaciones/ Hallazgos	% Implementación
14.2.9 PRUEBA DE ACEPTACIÓN DE SISTEMAS	¿Se tienen definidos controles y criterios para la aceptación de aplicaciones propias o contratadas por clientes?	No	N/A	0%
14.3	**DATOS DE PRUEBA**			
14.3.1 PROTECCIÓN DE DATOS DE PRUEBA	¿Cómo se asegura la protección de los datos usados para pruebas?	No Aplica	N/A	No Aplica
15	**RELACIONES CON LOS PROVEEDORES**			
15.1	**SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES**			
15.1.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES	¿Están documentados los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos?	No están documentados	N/A	0%
15.1.2 TRATAMIENTO DE LA SEGURIDAD DENTRO DE LOS ACUERDOS CON PROVEEDORES	¿Se han establecido requisitos de seguridad de la información con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura IT??	En proveedor no tiene acceso a la información. No hay acuerdo de confidencialidad	N/A	20%
15.1.3 CADENA DE SUMINISTRO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN	¿Los acuerdos de confidencialidad con terceros incluyen el tratamiento de riesgos asociado con la operación??	No Aplica	N/A	No Aplica

Cuadro 1. (Continuación)

Criterio ISO 27001:2013	Descripción	Comentarios para el Auditor y saber que temas debe tener en cuenta para preguntar o para el Auditado y preparar la auditoría	Observaciones/ Hallazgos	% Implementación
15.2	**GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE PROVEEDORES**			
15.2.1 SEGUIMIENTO Y REVISIÓN DE LOS SERVICIOS DE LOS PROVEEDORES	¿Cómo y con qué frecuencia realiza el seguimiento, revisión y auditoría a la prestación de servicios de los proveedores?	Se aplican procesos de revisión	No está definida una política o algún tipo de auditoría	20%
15.2.2 GESTIÓN DE CAMBIOS EN LOS SERVICIOS DE LOS PROVEEDORES	¿Se gestionan los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes?	No se hace esta gestión	No hay SGSI	0%
16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**			
16.1	**GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN**			
16.1.1 RESPONSABILIDADES Y PROCEDIMIENTOS	¿Se tiene establecida una política en la que se incluyan responsabilidades y procedimientos para la gestión de incidentes?	No hay manejo de incidente	N/A	0%
16.1.2 REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN	¿Se informa oportunamente la ocurrencia de incidentes de seguridad de la información a través de los canales de comunicación establecidos?	Evidenciar el procedimiento para reportar eventos de seguridad de la información y el punto de contacto al que se deberían reportar los eventos, según lo haya definido la organización.	No tienen definido que es un incidente de seguridad y no han informado a los funcionarios como realizar el reporte de estos incidentes.	0%
16.1.3 REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	¿De qué manera se exige a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios?	No han ocurrido, pero no se tiene contemplada la posibilidad	N/A	0%
16.1.4 EVALUACIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN Y DECISIONES SOBRE ELLOS	¿Se tiene una metodología para decidir si un evento de seguridad se considera como un incidente de seguridad?	No	N/A	0%
16.1.5 RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	¿Se tiene definido un procedimiento de atención de incidentes de seguridad?	No	N/A	0%

Cuadro 1. (Continuación)

Criterio ISO 27001:2013	Descripción	Comentarios para el Auditor y saber que temas debe tener en cuenta para preguntar o para el Auditado y preparar la auditoría	Observaciones/ Hallazgos	% Implementación
16.1.6 APRENDIZAJE OBTENIDO DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	¿Se hace uso de las lecciones aprendidas para mejorar los procedimientos de atención de incidentes de seguridad de la información??	No	N/A	0%
16.1.7 RECOLECCIÓN DE EVIDENCIA	¿Se tiene definido un procedimiento para la identificación, recolección y preservación de evidencia originada por un incidente de seguridad de la información??	No	N/A	0%
17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO**			
17.1	**CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN**			
17.1.1 PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	¿Se tiene definido una política o procedimiento que permita a la organización continuar su operación tras la ocurrencia de eventos que impidan su normal funcionamiento??	No se tiene definido un SGSI, y poca información hay relacionada a la seguridad de la información	N/A	0%
17.1.2 IMPLEMENTACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	¿Se han establecido, documentado, implementado y se mantienen procesos, procedimientos y controles que permitan la continuidad del negocio??	No	N/A	0%
17.1.3 VERIFICACIÓN, REVISIÓN Y EVALUACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	¿Se verifica con periodicidad la política, procedimientos o controles con el objetivo de determinar que se encuentran de acuerdo con las necesidades de la organización??	No	N/A	0%
17.2	**REDUNDANCIAS**			
17.2.1 DISPONIBILIDAD DE INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN	¿Se tienen controles e infraestructura que permitan mantener la continuidad de operación de la organización?	No	N/A	0%

Cuadro 1. (Continuación)

Criterio ISO 27001:2013	Descripción	Comentarios para el Auditor y saber que temas debe tener en cuenta para preguntar o para el Auditado y preparar la auditoría	Observaciones/ Hallazgos	% Implementación
18	**CUMPLIMIENTO**			
18.1	**CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES**			
18.1.1 IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE Y DE LOS REQUISITOS CONTRACTUALES	¿Qué documentación recopila todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos?	Requisitos contractuales identificados por la organización.	N/A	60%
18.1.2 DERECHOS DE PROPIEDAD INTELECTUAL	¿Qué procedimientos tiene implementados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados?	Si, se cuenta con el sistema de gestión de calidad	N/A	40%
18.1.3 PROTECCIÓN DE REGISTROS	¿Se han implementado políticas y procedimientos para la protección de la información contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada?	No	N/A	0%
18.1.4 PRIVACIDAD Y PROTECCIÓN DE INFORMACIÓN DE DATOS PERSONALES	¿Se han implementado políticas y controles que permitan mantener la privacidad y la protección de la información de datos personales, de acuerdo a la normatividad vigente?	No	N/A	0%
18.1.5 REGLAMENTACIÓN DE CONTROLES CRIPTOGRÁFICOS	¿Se usan controles criptográficos en la organización, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes?	No	N/A	0%

Cuadro 1. (Continuación)

Criterio ISO 27001:2013	Descripción	Comentarios para el Auditor y saber que temas debe tener en cuenta para preguntar o para el Auditado y preparar la auditoría	Observaciones/ Hallazgos	% Implementación
18.2	**REVISIONES DE SEGURIDAD DE LA INFORMACIÓN**			
18.2.1 REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN	¿Cómo y con qué frecuencia se revisa el enfoque de la seguridad de la información y su implementación en la organización?	No se hace la revisión porque no hay política de seguridad de la información, ni SGSI	N/A	0%
18.2.2 CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD	¿Se revisa por parte de la gerencia el cumplimiento de la normatividad vigente respecto a la seguridad de la información?	No se hace la revisión porque no hay política de seguridad de la información, ni SGSI	N/A	0%
18.2.3 REVISIÓN DEL CUMPLIMIENTO TÉCNICO	¿Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información?	No se hace la revisión porque no hay política de seguridad de la información, ni SGSI	N/A	0%
Observaciones				

N/A No Aplica

Firma Auditor Líder

* NOTA: EL control 12.2.1 No se tiene en cuenta, porque la empresa no realiza ningún tipo de desarrollo, por lo tanto, no aplica

Fuente: Autores. Información suministrada por Acceso Directo Asociados Limitada.

El resultado de la revisión fue tabulado en tablas de calificación para facilitar su interpretación.

Llevado a cabo el análisis de las respuestas e identificando los hallazgos, evidencias, controles y partiendo de un criterio de análisis al cuestionario definido en el mismo formato, se puede ver la calificación que refleja el nivel de cumplimiento de la empresa Acceso Directo Asociados Limitada, respecto a la norma ISO 27001:2013, en el Cuadro 2. Promedio de calificación numerales 4 al 10 norma ISO 27001:2013. se evidencia el resultado con respecto a los numerales del 4 al 10 de la norma ISO 27001:2013 el cual corresponde a un 3% de cumplimiento total respecto a los dominios de la norma, el 97% restante corresponde a incumplimientos, procesos existentes no documentados, cumplimientos parciales o en casos puntuales numerales que no aplican a los requerimientos de seguridad de la información definidos en el anexo A de la norma ISO 27001:2013.

Cuadro 2. Promedio de calificación numerales 4 al 10 norma ISO 27001:2013.

Promedio de la calificación de las preguntas a los numerales 4 a 10 de norma ISO 27001:2013		
Numeral evaluado		**Calificación**
4	Contexto de la Organización	10%
5	Liderazgo	8%
6	Planificación	0%
7	Soporte	4%
8	Operación	0%
9	Evaluación del desempeño	0%
10	Mejora	0%
	Nivel de seguridad	3%
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.		

En el Cuadro 3. Promedio de calificación anexo A norma ISO 27001:2013 se evidencia el resultado con respecto al Anexo A de la norma ISO 27001:2013 el cual corresponde a un 7% de cumplimiento total respecto a los controles del Anexo A de la norma, el 93% restante corresponde a incumplimientos, procesos existentes no documentados, cumplimientos parciales o en casos puntuales numerales que no aplican a los requerimientos de seguridad de la información definidos en el anexo A de la norma ISO 27001:2013.

Cuadro 3. Promedio de calificación anexo A norma ISO 27001:2013

Promedio de la calificación de las preguntas a los dominios del anexo A de la norma ISO 27001:2013		
Dominio evaluado		**Calificación**
A5	Políticas de seguridad	0%
A6	Organización de seguridad de la información	0%
A7	Seguridad de los recursos humanos	23%
A8	Gestión de los activos	18%
A9	Control de acceso	3%
A10	Criptografía	0%
A11	Seguridad física y del entorno	15%
A12	Seguridad de las operaciones	14%
A13	Seguridad de las comunicaciones	9%
A14	Adquisición, desarrollo y mantenimiento de SI	0%
A15	Relaciones con los proveedores	10%
A16	Gestión de incidentes de seguridad de la Información	0%
A17	Gestión de continuidad del negocio	0%
A18	Cumplimiento	13%
	Nivel de seguridad	7%
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada		

En el Cuadro 4. Identificación de brecha se puede ver el cumplimiento general de los dominios del anexo A de la norma ISO 27001:2013, donde se miden los cumplimientos en porcentajes del 0 al 100% el cual deja en evidencia que la empresa Acceso Directo Asociados Limitada, tiene porcentajes de cumplimiento muy bajos con respecto a la norma, dichos numerales serán desglosados uno por uno en el documento.

6.2.1.4 Objetivos a conseguir. El cumplimiento de los objetivos es netamente decisión de la empresa Acceso Directo Asociados Limitada, ya que la fase de implementación se encuentra fuera del alcance de este proyecto.

Con respecto a los resultados obtenidos de la revisión, en el diseño se plantea como objetivo el cumplimiento de la totalidad de los requisitos y controles, si bien no se podría asegurar que en un 100% sea un porcentaje de riesgo aceptable, para el caso particular de la empresa se ha puesto un umbral del 85%, aclarando que los dominios referentes a auditorías y mejora continua no son de cumplimiento

en esta primera fase y quedan sujetos a disposición de la empresa Acceso Directo Asociados Limitada.

6.2.1.5 Identificación de brecha. La diferencia obtenida entre el estado actual y el estado de cumplimiento esperado da como resultado la cantidad de esfuerzo que será aplicado para lograr el objetivo esperado en el diseño y posterior implementación de un Sistema de Gestión de Seguridad de la Información SGSI para la empresa Acceso Directo Asociados Limitada.

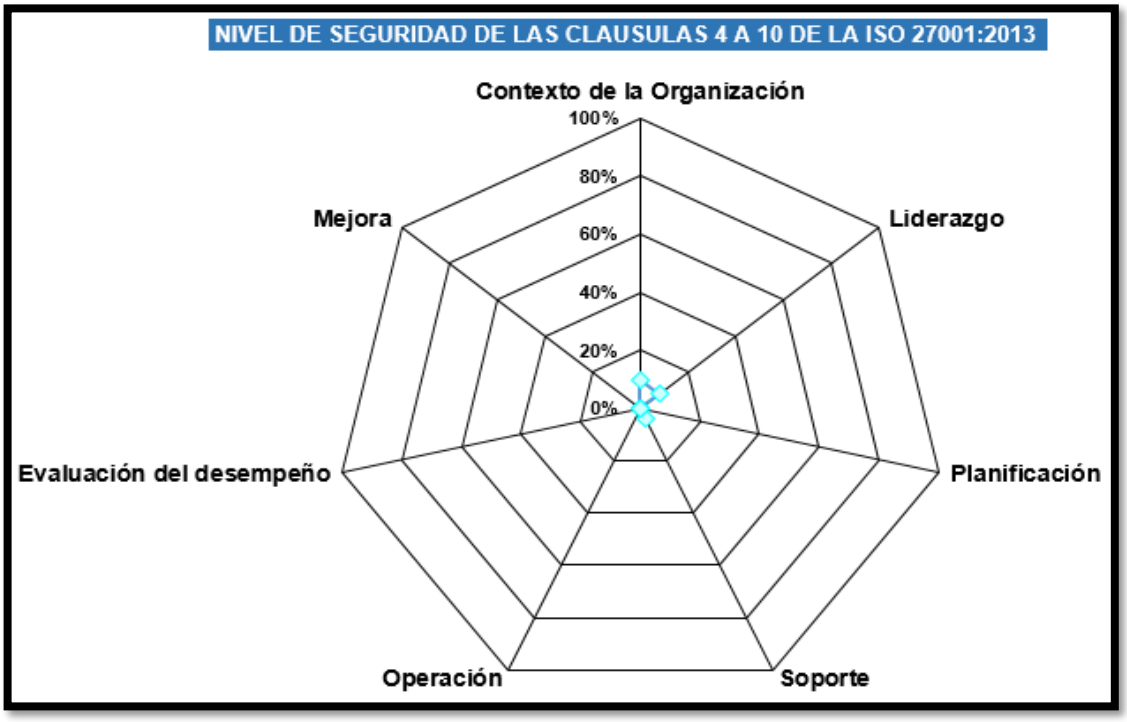
Cuadro 4. Identificación de brecha

Norma ISO 27001:2013	Estado actual	Estado esperado	Diferencia
Dominios 4 al 10	3%	85%	82%
Anexo A	7%	85%	78%
Fuente: Autores.			

6.2.2 Detalle requisitos de la norma ISO 27001:2013. La siguiente información es un análisis detallado de los requisitos y controles de los numerales 4 al 10 de la norma ISO 27001:2013 y el anexo A de la misma.

6.2.2.1 Cumplimiento de los controles de los numerales del 4 al 10 de la norma ISO 27001:2013. En la Gráfica 2. Promedio de calificación numerales 4 al 10 norma ISO 27001:2013 se evidencia el nivel de seguridad de las cláusulas 4 a 10 de la norma aplicada.

Gráfica 2. Promedio de calificación numerales 4 al 10 norma ISO 27001:2013



Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.

a. **Contexto de la organización:** Se realizó el proceso de identificación de factores tanto internos como externos que tienen algún tipo de impacto sobre el objetivo del negocio, estos incluyen clientes, proveedores, competencia, proyectos en ejecución y por ejecutar; El hecho de que la seguridad de la información es un requisito y para este caso en especial una necesidad puesto que el conocimiento de la seguridad informática en la empresa está muy por debajo de los niveles que se consideran aceptables.

Gráfica 3. Promedio calificación, contexto de la organización norma ISO 27001:2013

Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.

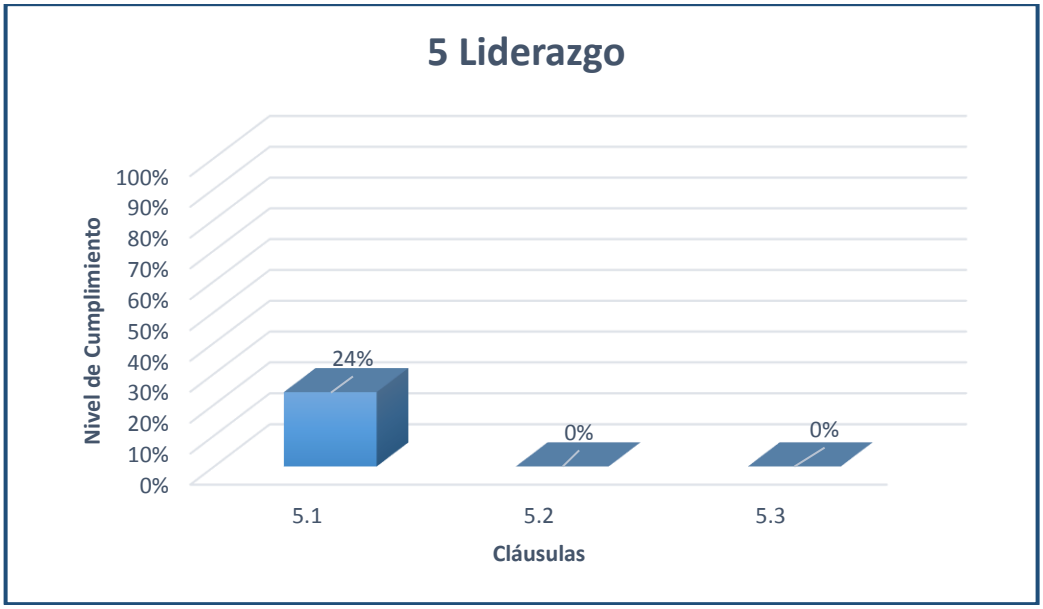
Cuadro 5. Cláusulas contexto de la organización

Cláusulas	
4.1	Conocimiento de la organización y su contexto
4.2	Comprensión de las necesidades y expectativas de las partes interesadas
4.3	Determinación del alcance del sistema de gestión de la seguridad de la información
4.4	Sistema de gestión de la seguridad de la información
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada	

b. Liderazgo: Las áreas directamente participantes de la empresa como lo son la gerencia y la oficina de sistemas tienen conocimiento y plena conciencia de que la seguridad informática es una necesidad para ellos, se evidencian las falencias principales, como la documentación, las políticas y la falta de dirección de los procesos que en el momento se aplican.

Como parte del apoyo al proceso del diseño del SGSI para la empresa acceso directo, la gerencia ha dispuesto de los recursos de información sobre procesos específicos y un recurso humano en la oficina de sistemas (jefe de la oficina), para llevar a cabo este proceso.

Gráfica 4. Promedio calificación, liderazgo norma ISO 27001:2013



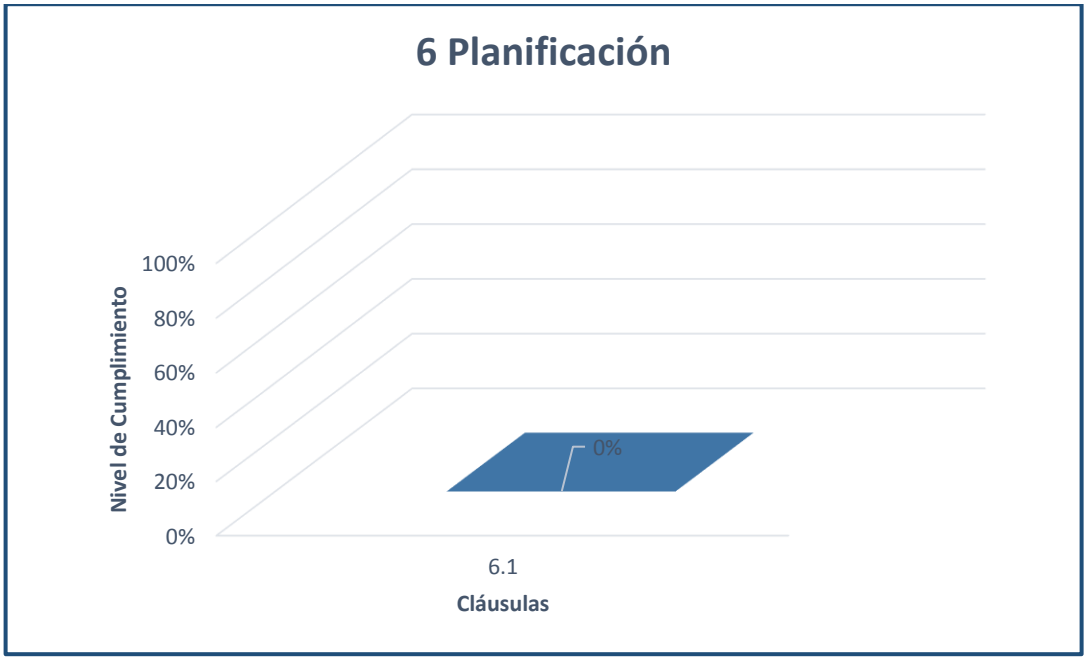
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.

Cuadro 6. Cláusulas Liderazgo

Cláusulas	
5.1	Liderazgo y compromiso
5.2	Política
5.3	Roles, responsabilidades y autoridades en la organización.
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.	

c. Planificación: se identifica la necesidad de llevar a cabo un análisis de vulnerabilidades sobre los componentes de la infraestructura informática de Acceso Directo Asociados Limitada, ya que al día de hoy no se cuenta con ningún análisis de este tipo que permita identificar el nivel de vulnerabilidad frente a amenazas a los dispositivos informáticos y la información.

Gráfica 5. Promedio calificación, planificación norma ISO 27001:2013



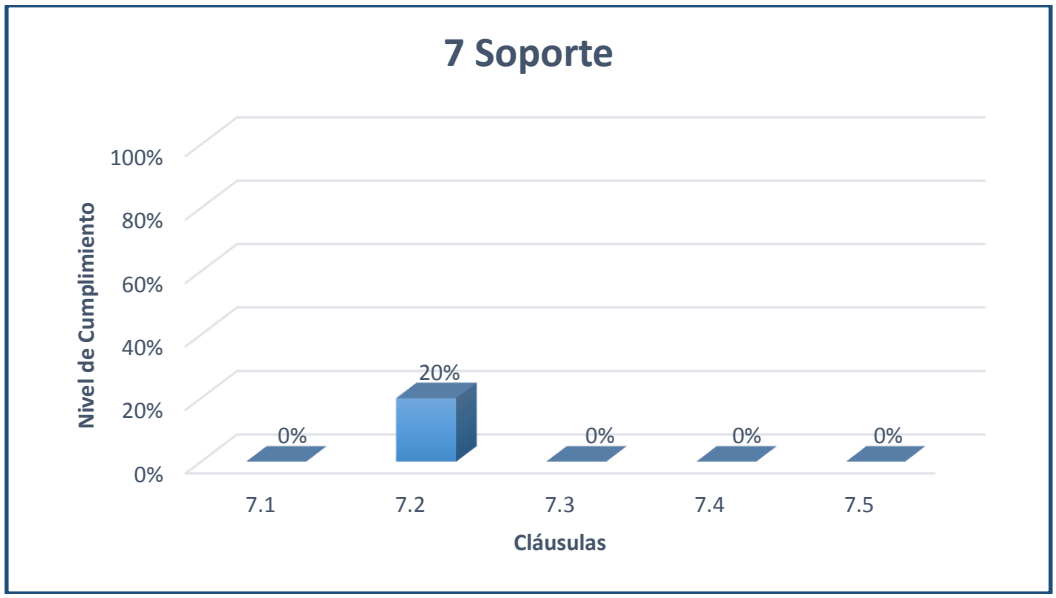
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.

Cuadro 7. Cláusulas planificación

Cláusulas	
6.1	Acciones para tratar riesgos y oportunidades
6.2	Objetivos de seguridad de la información y planes para lograrlo
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.	

d. Soporte: Debido a que la empresa no cuenta con políticas definidas, ni procedimientos de seguridad documentados, la mayoría de los funcionarios de la empresa no conocen instrucciones o lineamientos sobre los procesos adecuados para dar cumplimiento a los estándares de seguridad de la información.

Gráfica 6. Promedio calificación, soporte norma ISO 27001:2013



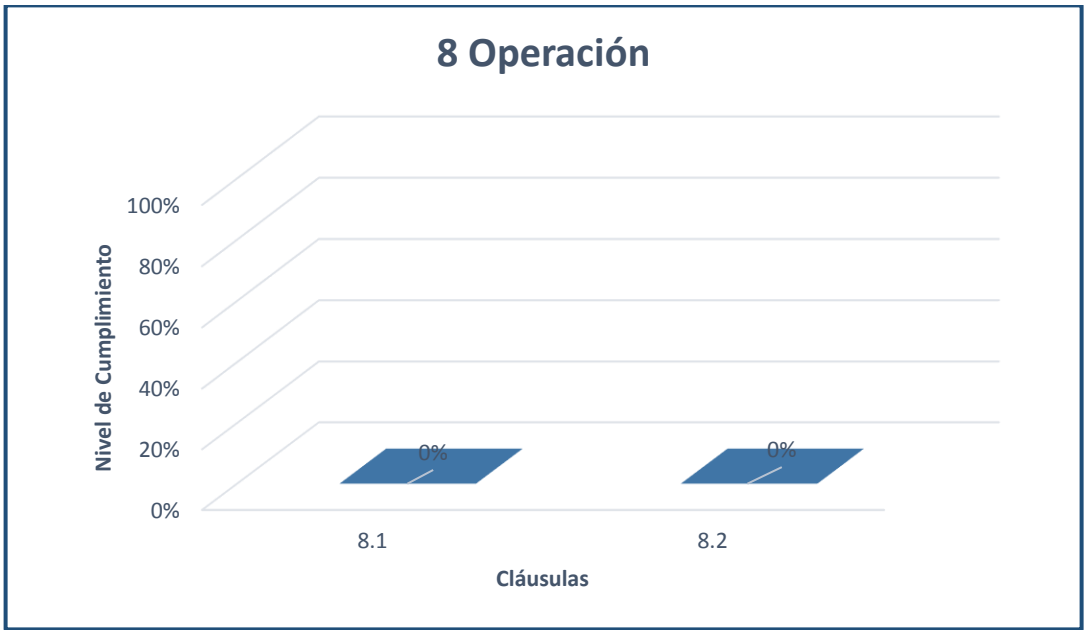
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.

Cuadro 8. Cláusulas soporte

Cláusulas	
7.1	Recursos
7.2	Competencia
7.3	Toma de conciencia
7.4	Comunicación
7.5	Información documentada
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.	

e. Operación: El proceso de mejora continua no está contemplado, debido a que sin existir una implementación, políticas o tratamiento de riesgos no hay ninguna medición que permita llevar un proceso de mejora.

Gráfica 7. Promedio calificación, operación norma ISO 27001:2013



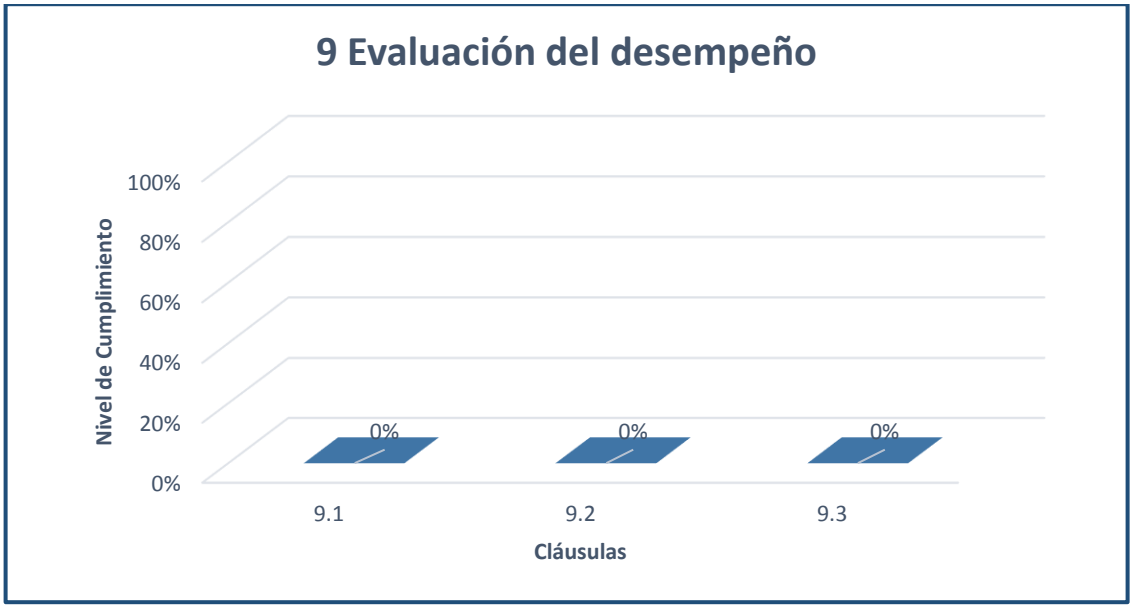
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.

Cuadro 9. Cláusulas operación

Cláusulas	
8.1	Planificación y control operacional
8.2	Valoración de riesgos de seguridad de la información
8.3	Tratamiento de riesgos de la seguridad de la información
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.	

f. Evaluación del desempeño: no es posible llevar a cabo una evaluación de desempeño como tal, ya que al no estar documentado ningún proceso de seguridad de la información, no existe ninguna actividad sobre la cual medir el desempeño.

Gráfica 8. Promedio calificación, evaluación de desempeño norma ISO 27001:2013.



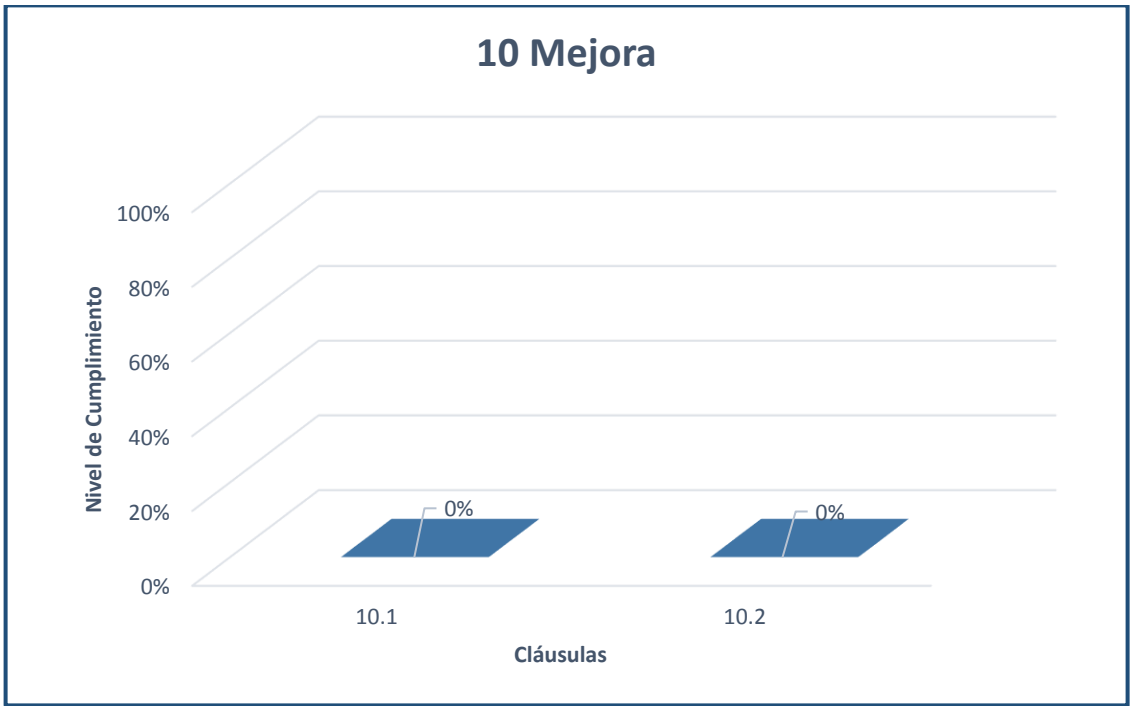
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.

Cuadro 10. Cláusulas evaluación del desempeño

Cláusulas	
9.1	Seguimiento, medición, análisis y evaluación
9.2	Auditoría interna
9.3	Revisión por la dirección
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.	

g. Mejora: No hay ninguna actividad definida sobre la cual se pueda hacer mediciones para generar un plan de mejora.

Gráfica 9. Promedio calificación, mejora norma ISO 27001:2013.



Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.

Cuadro 11. Cláusulas mejora

Cláusulas	
10.1	No conformidades y acciones correctivas
10.2	Mejora continua
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.	

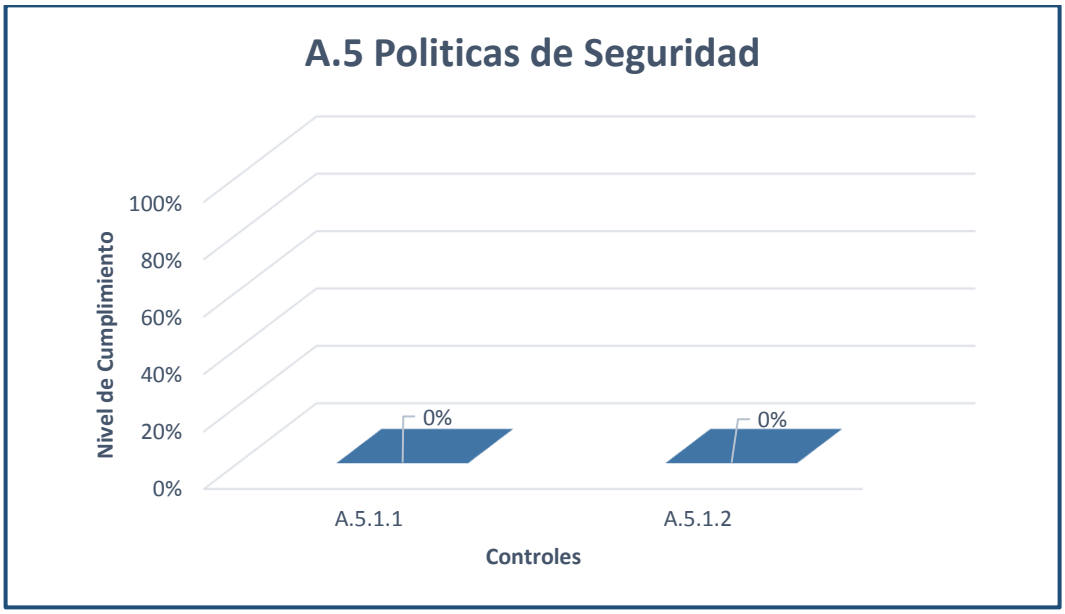
6.2.2.2 Cumplimiento de los controles del Anexo A de la norma ISO 27001:2013.

Gráfica 10. Promedio calificación anexo A norma ISO 27001:2013

Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.

A.5 Políticas de Seguridad: Este numeral no se cumple, en la Gráfica 11. Numeral A.5 anexo A norma ISO 27001:2013 se puede observar que los numerales secundarios que se desprenden se encuentran en un nivel de cumplimiento de 0%, esto debido a que no existe una política definida, ni documentada por lo tanto tampoco se han hecho los procesos de aprobación y divulgación de la política por parte de la gerencia.

Gráfica 11. Numeral A.5 anexo A norma ISO 27001:2013



Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.

Cuadro 12. Controles de políticas de seguridad

Controles	
A.5.1.1	Políticas para la seguridad de la información
A.5.1.2	Revisión de las políticas para seguridad de la información
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.	

A.6 Organización de Seguridad de la información: En la empresa no se tiene definida un área de seguridad de la información, tampoco una persona que se encargue de los procesos (no documentados) que se llevan a cabo, el personal de la oficina de sistemas se dedica solamente a cosas del común en TI, como: computadores, equipos de red, servidores, pagina web.

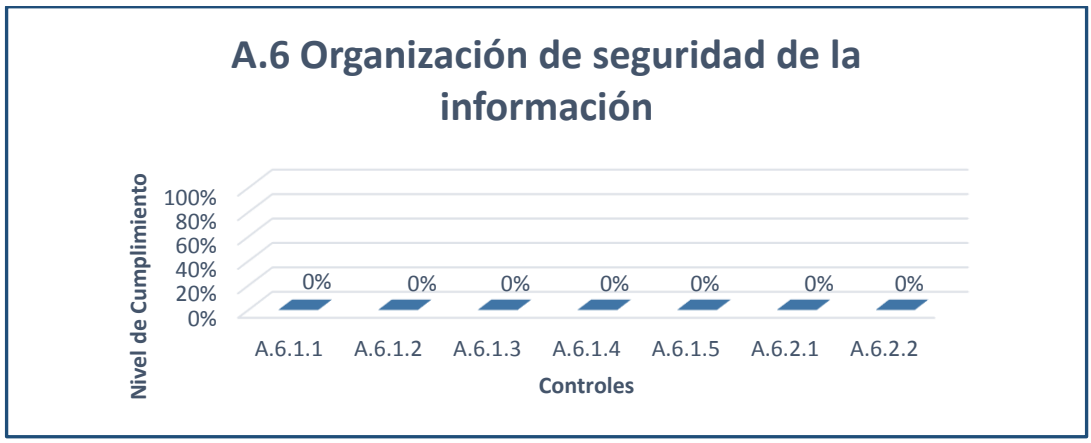
La empresa Acceso Directo Asociados Limitada, está dedicada a comunicación y publicidad no se rige por ninguna normatividad o autoridad especial, por lo tanto, no se contemplan leyes generales de protección de datos personales.

La responsabilidad en cuanto al cumplimiento de la normatividad relacionada, está directamente sobre la gerencia de la empresa, se contempla la aplicabilidad de está en cuanto al impacto directo con la empresa y las consecuencias del cumplimiento o no de las mismas.

Como lo evidencia la Gráfica 12. Numeral A.6 anexo A norma ISO 27001:2013 que se encuentra a continuación, todos los numerales secundarios del numeral de 6 del anexo A se encuentran en un nivel de cumplimiento y ejecución de 0% por lo tanto no se vislumbra contacto con otras entidades, ni grupos de interés.

Tampoco se cuenta con ninguna política para dispositivos móviles, a pesar de que los únicos dispositivos móviles que se usan en la empresa son personales no se debe descartar una política para el uso de los mismos, el teletrabajo no está contemplado por el momento en Acceso Directo Asociados Limitada.

Gráfica 12. Numeral A.6 anexo A norma ISO 27001:2013



Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.

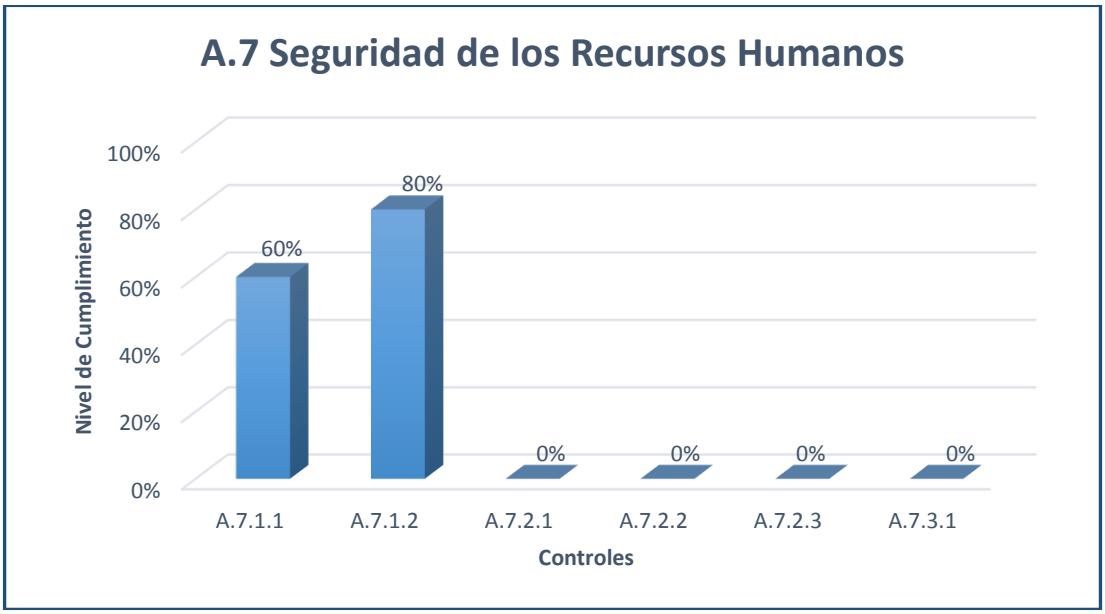
Cuadro 13. Controles organización de seguridad de la información

Controles	
A.6.1.1	Roles y responsabilidades para la seguridad de la información
A.6.1.2	Separación de deberes
A.6.1.3	Contacto con las autoridades
A.6.1.4	Contacto con grupos de interés social
A.6.1.5	Seguridad de la información en la gestión de los proyectos
A.6.2.1	Política para dispositivos móviles
A.6.2.2	Teletrabajo
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.	

A.7 Seguridad de los recursos humanos: Se realizan las pruebas reglamentarias para asumir un empleo como las pruebas de conocimiento, las pruebas psicotécnicas y si es el caso una prueba sobre manejo de tecnologías de la información y la comunicación, se lleva a cabo la revisión de antecedentes fiscales al momento de ingresar a trabajar se hace la firma del acuerdo de confidencialidad adicional al contrato.

Una vez en ejecución del empleo no hay forma de hacer control o exigir que se cumpla con una política de seguridad de la información, debido a que esta no existe, no se llevan a cabo procesos de sensibilización ni de concienciación a los empleados, tampoco se encuentra definida una política o un proceso de cambio de funciones o terminación del contrato, solo un proceso sencillo de terminación del contrato y liquidación.

Gráfica 13. Numeral A.7 anexo A norma ISO 27001:2013



Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.

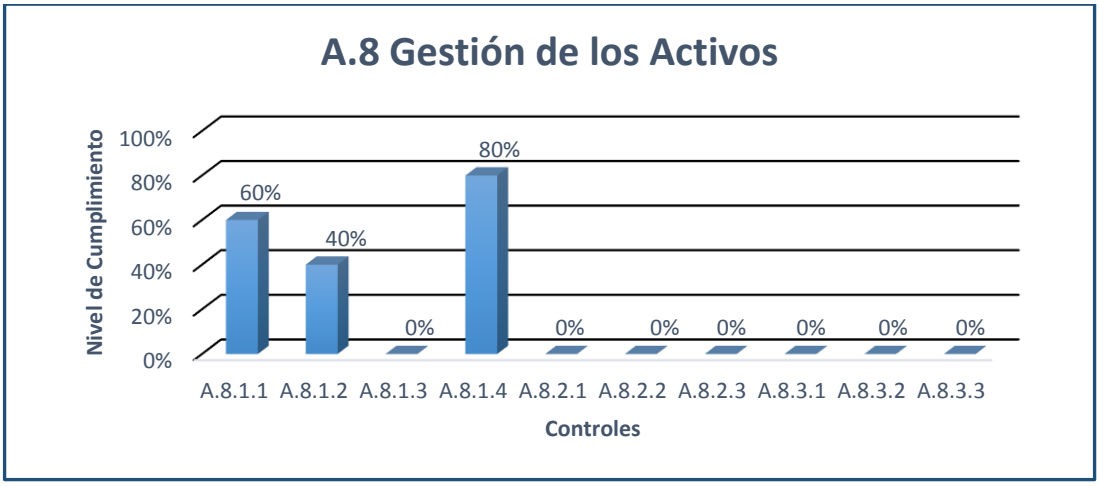
Cuadro 14. Controles seguridad de los recursos humanos

Controles	
A.7.1.1	Roles y responsabilidades
A.7.1.2	Términos y condiciones de empleo
A.7.2.1	Responsabilidades de la dirección
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información
A.7.2.3	Proceso disciplinario
A.7.3.1	Terminación o cambio de responsabilidades de empleo
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.	

A.8 Gestión de los Activos: La empresa cuenta con un inventario de equipos de cómputo, audiovisuales y demás activos que son propiedad de Acceso Directo Asociados Limitada, aunque no se cuenta con un inventario de activos de información que permitan dar cumplimiento a lo requerido por la norma ISO 27001:2013. La empresa cuenta con un proceso no documentado donde se asegura de alguna forma que los empleados regresen los activos que les han sido asignados.

No se tiene una política o procedimiento definido sobre clasificación y uso de la información donde se tenga en cuenta el nivel de confidencialidad de la misma según lo descrito en la normatividad, teniendo en cuenta los pilares de la seguridad informática como son, confidencialidad, integridad y disponibilidad. Tampoco cuenta con una política de medios removibles, no se han definido restricciones sobre medios de almacenamiento extraíbles por parte de los funcionarios de Acceso Directo Asociados Limitada y tampoco se tiene un documento claro sobre qué personal está autorizado a utilizar qué tipo de información.

Gráfica 14. Numeral A.8 anexo A norma ISO 27001:2013



Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.

Cuadro 15. Controles gestión de los activos

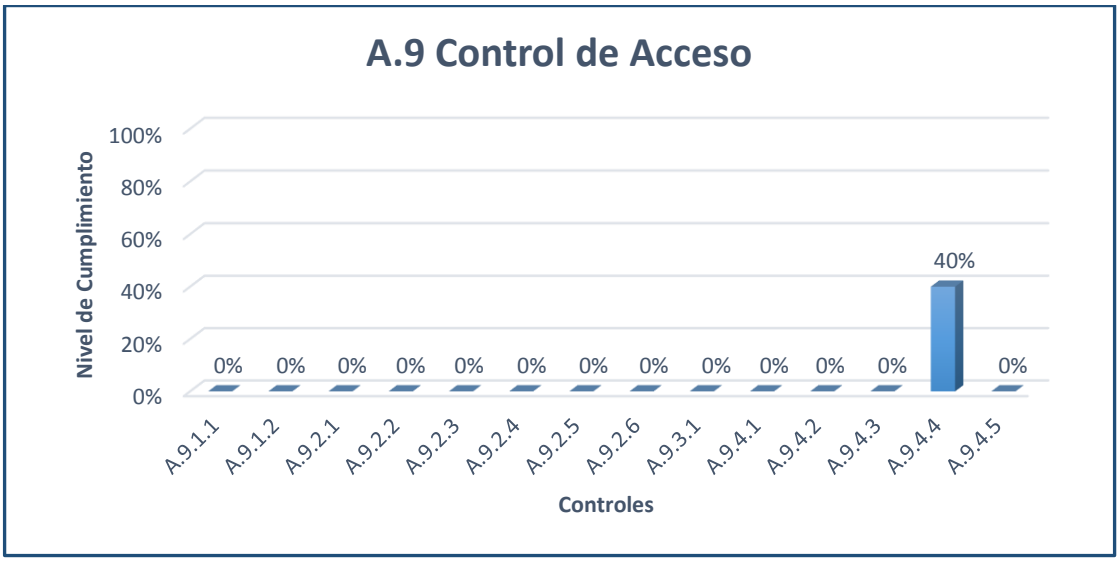
Controles	
A.8.1.1	Inventario de activos
A.8.1.2	Propiedad de los activos
A.8.1.3	Uso aceptable de los activos
A.8.1.4	Devolución de los activos
A.8.2.1	Clasificación de la información
A.8.2.2	Etiquetado de la información
A.8.2.3	Manejo de activos
A.8.3.1	Gestión de medios removibles
A.8.3.2	Disposición de los medios
A.8.3.3	Transferencia de medios físicos
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.	

A.9 Control de Acceso: Las directrices de control de acceso en la empresa no se encuentran definidas, en su mayoría los numerales secundarios tienen un porcentaje de cumplimiento de 0%, en cuanto a la información, no está almacenada en un lugar restringido y seguro.

El sistema de creación de usuarios y contraseñas de acceso al sistema de información no está definido, en el área de sistemas hay una persona encargada de supervisar el acceso, sin embargo, sin un procedimiento o política establecida es un control superficial. Tampoco se cuenta con ningún tipo de procedimiento para reasignar funciones, modificar o quitar privilegios, para esto es necesario en primer lugar definir un sistema de usuarios de dominio.

El software utilizado es licenciado, se usa software propietario comprado directamente a desarrolladores, puesto que la empresa no maneja ningún tipo de desarrollo propietario.

Gráfica 15. Numeral A.9 anexo A norma ISO 27001:2013



Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.

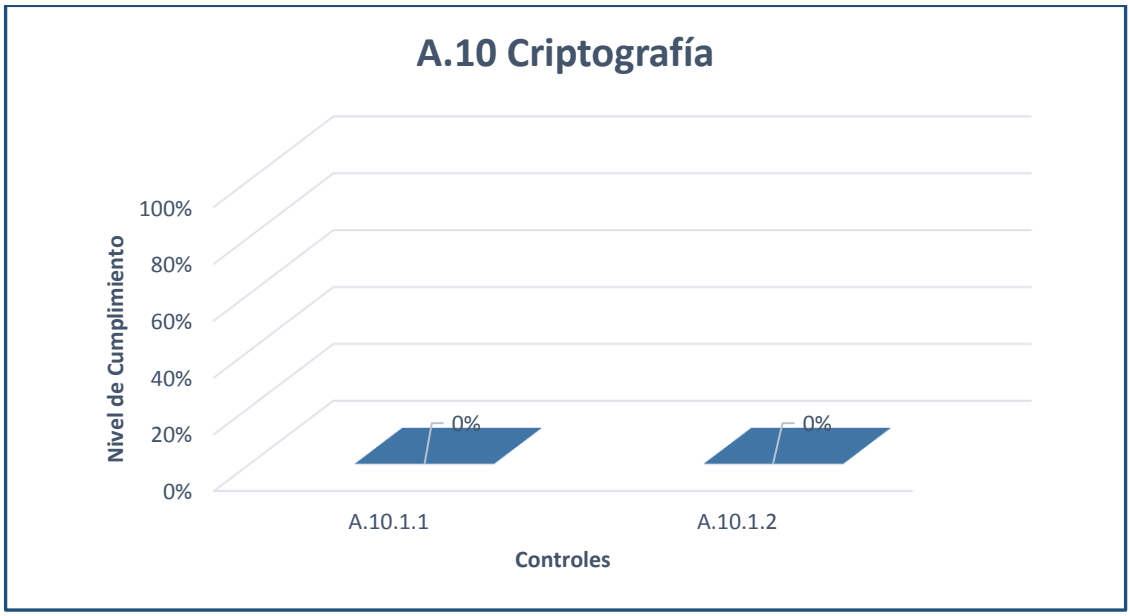
Cuadro 16. Controles control de acceso

Controles	
A.9.1.1	Política de control de acceso
A.9.1.2	Acceso a redes y a servicios en red
A.9.2.1	Registro y cancelación del registro de usuarios
A.9.2.2	Suministro de acceso de usuarios
A.9.2.3	Gestión de derechos de acceso privilegiado
A.9.2.4	Gestión de información de autenticación secreta de usuarios
A.9.2.5	Revisión de los derechos de acceso de usuarios
A.9.2.6	Retiro o ajuste de los derechos de acceso
A.9.3.1	Uso de información de autenticación secreta
A.9.4.1	Restricción de acceso a la información
A.9.4.2	Procedimiento de ingreso seguro
A.9.4.3	Sistema de gestión de contraseñas
A.9.4.4	Uso de programas utilitarios privilegiados
A.9.4.5	Control de acceso a códigos fuente de programas
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.	

A.10 Criptografía: No hay ninguna política sobre el uso de controles criptográficos, la empresa Acceso Directo Asociados Limitada no utiliza ningún tipo de llave criptográfica, el intercambio de información se lleva a cabo generalmente a través de correos electrónicos, pero estos no llevan ningún tipo de algoritmo de cifrado.

No se usa ningún tipo de VPN, ni virtualización de red, las conexiones en remoto se hacen a través de aplicaciones integradas de software como escritorio remoto o por medio de software como teamviewer.

Gráfica 16. Numeral A.10 anexo A norma ISO 27001:2013.



Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.

Cuadro 17. Controles criptografía

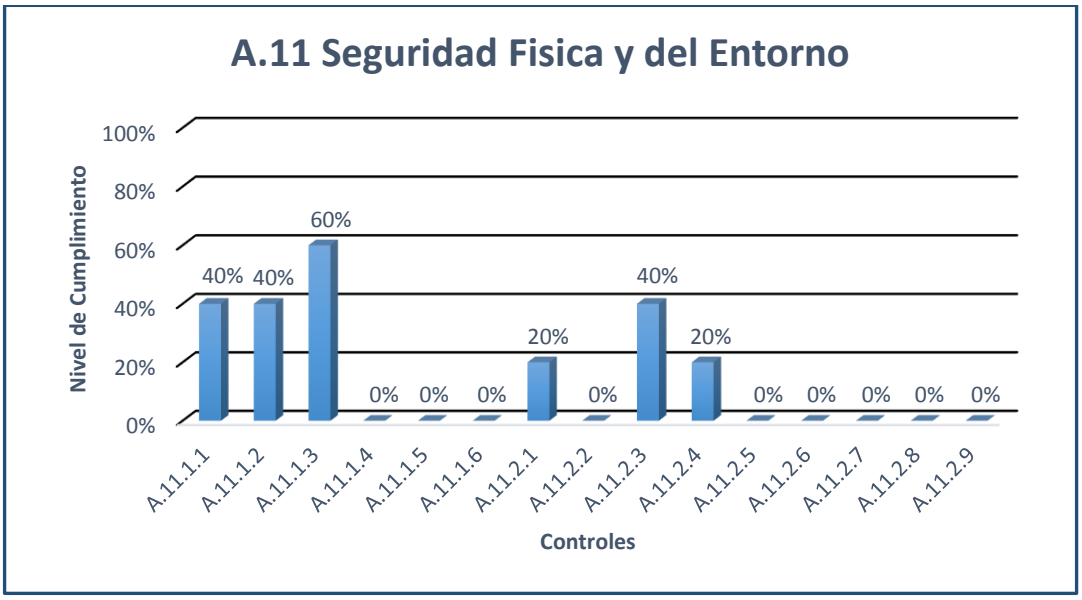
Controles	
A.10.1.1	Política sobre el uso de controles criptográficos
A.10.1.2	Gestión de llaves
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.	

A.11 Seguridad física y del entorno: La empresa no cuenta con ningún tipo de área restringida, las oficinas más importantes como la de la gerencia se encuentran aseguradas con llaves, sin embargo, el espacio donde están dispuestos los servidores no cuenta con ningún tipo de seguridad ni restricción de acceso a usuarios, la seguridad perimetral está a cargo del edificio, se cuenta con un vigilante en la portería principal de acceso al edificio, adicional a esto la empresa tiene un sistema de CCTV al interior de las instalaciones.

No hay ninguna política de usuarios y contraseñas para proteger los equipos de accesos no autorizados, algunos de los equipos portátiles no cuentan con guayas, ni sistemas de bloqueo automático, en casos específicos los portátiles deben ser retirados de la empresa, esto no queda en ningún registro.

No se cuenta con redundancia ni protección eléctrica para los servidores, tampoco hay soporte a nivel de red de datos e internet, si por algún motivo llega a fallar, la empresa quedaría sin funcionamiento hasta que se restablezca el servicio; tampoco se cuenta con un plan de mantenimiento, solo se realiza mantenimiento correctivo, en ningún caso se hace mantenimiento preventivo programado, no existen políticas de almacenamiento de información, modificación de la misma o técnicas de borrado seguro, no hay documentado ningún proceso sobre almacenamiento en medios extraíbles, ni una política de escritorio limpio.

Gráfica 17. Numeral A.11 anexo A norma ISO 27001:2013



Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.

Cuadro 18. Controles seguridad física y del entorno

Controles	
A.11.1.1	Perímetro de seguridad física
A.11.1.2	Controles físicos de entrada
A.11.1.3	Seguridad de oficinas, recintos e instalaciones
A.11.1.4	Protección contra amenazas externas y ambientales
A.11.1.5	Trabajo en áreas seguras
A.11.1.6	Áreas de despacho y carga
A.11.2.1	Ubicación y protección de los equipos
A.11.2.2	Servicios de suministro
A.11.2.3	Seguridad del cableado
A.11.2.4	Mantenimiento de equipos
A.11.2.5	Retiro de activos
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones
A.11.2.7	Disposición segura o reutilización de equipos
A.11.2.8	Equipos de usuario desatendidos
A.11.2.9	Política de escritorio limpio y pantalla limpia
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.	

A.12 Seguridad de las operaciones: Los procedimientos no se encuentran documentados, ni publicados, la definición de responsabilidades tampoco está definida en la empresa Acceso Directo Asociados Limitada.

La empresa no hace ningún tipo de desarrollo propio por lo tanto el numeral 12.2.1 no aplica para este caso, tampoco es necesario aplicar medidas de protección contra códigos maliciosos porque no hay ningún proyecto al que se deba aplicar.

Se realizan copias de respaldo cada 15 días en discos duros externos, sin embargo, su almacenamiento no es el adecuado, ni está asegurado de ninguna forma, los discos duros reposan en la oficina de sistemas y tampoco se realiza ningún informe o acta posterior a la copia, respecto a la información confidencial o crítica no hay un responsable de la copia, esta copia se realiza en los mismos discos duros por la misma persona.

No hay ningún procedimiento o proceso definido de control de registros en los sistemas, ni actividades de funcionarios o comportamiento del servidor, tampoco hay una persona responsable de hacer el seguimiento o auditoría de los sistemas

de información por lo tanto es difícil identificar algún tipo de modificación, alteración o eliminación de registros o información importante.

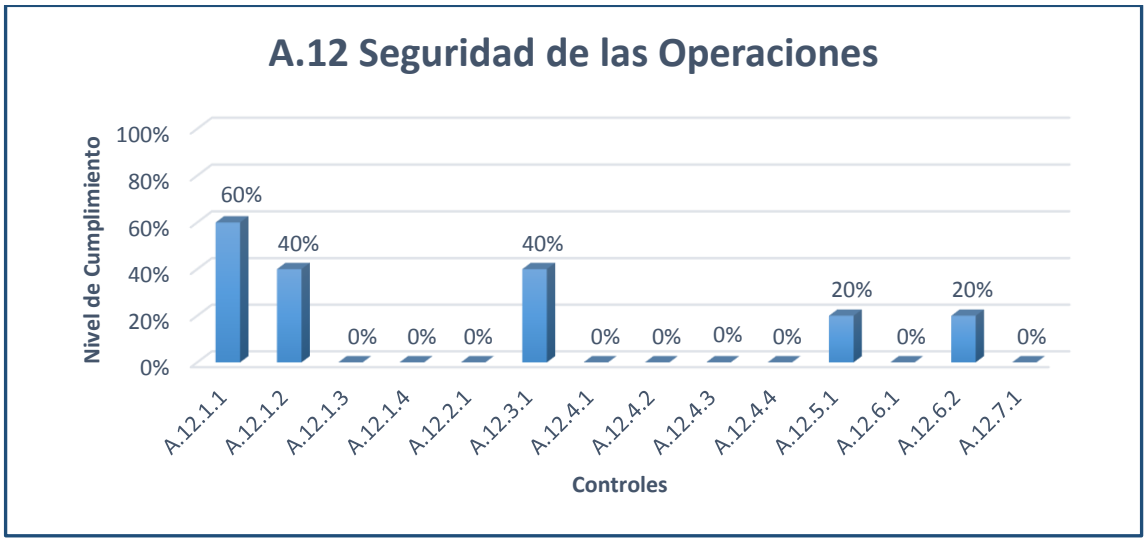
El único control efectivo que se lleva sobre la instalación de software es que se debe hacer en la oficina de sistemas, sin embargo, no hay ningún tipo de documentación al respecto.

Respecto a la gestión de vulnerabilidades la empresa Acceso Directo Asociados Limitada, no ha realizado ninguna prueba a los componentes de la infraestructura informática, por lo tanto, no se puede determinar la existencia o no de vulnerabilidades referentes a sistemas operativos o hardware y software en general para determinar si hay alguna amenaza que pueda afectar la seguridad de la información.

En cuanto a la instalación, reproducción o manipulación de software hay algunas restricciones desde la oficina de sistemas las cuales son dadas a conocer simplemente en forma verbal, no existe documentación al respecto, ni tampoco una política definida.

El tema de auditorías al sistema de información no se lleva a cabo en la empresa Acceso Directo Asociados Limitada, no se tienen contempladas auditorías donde se pueda identificar el cumplimiento en cuanto a los lineamientos de seguridad de la información.

Gráfica 18. Numeral A.12 anexo A norma ISO 27001:2013



Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.

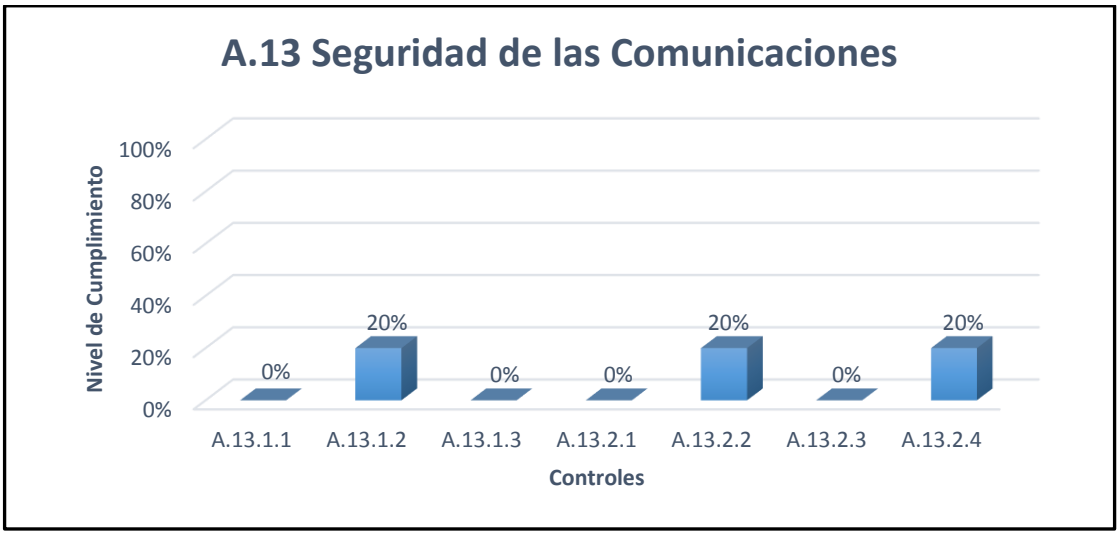
Cuadro 19. Controles seguridad de las operaciones

Controles	
A.12.1.1	Procedimientos de operación documentados
A.12.1.2	Gestión de cambios
A.12.1.3	Gestión de capacidad
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación
A.12.2.1	Controles contra códigos maliciosos
A.12.3.1	Respaldo de la información
A.12.4.1	Registro de eventos
A.12.4.2	Protección de la información de registro
A.12.4.3	Registros del administrador y del operador
A.12.4.4	Sincronización de relojes
A.12.5.1	Instalación de software en sistemas operativos
A.12.6.1	Gestión de vulnerabilidades técnicas
A.12.6.2	Restricciones sobre la instalación de software
A.12.7.1	Controles sobre auditorías de sistemas de información
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.	

A.13 Seguridad de las comunicaciones: No se tiene ninguna política, ni procedimiento definido para proteger la seguridad de la información en sistemas y aplicaciones, el intercambio de información se realiza a través de correo

electrónico, sin embargo, estos correos no manejan ningún tipo de cifrado, en caso de ser interceptados por algún tercero no autorizado su interpretación es posible, se lleva a cabo la firma de acuerdo de confidencialidad entre Acceso Directo Asociados Limitada pero no se asegura el cumplimiento de estos ya que no hay una supervisión definida puesto que estos acuerdos de confidencialidad son netamente verbales.

Gráfica 19. Numeral A.13 Anexo A norma ISO 27001:2013.



Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.

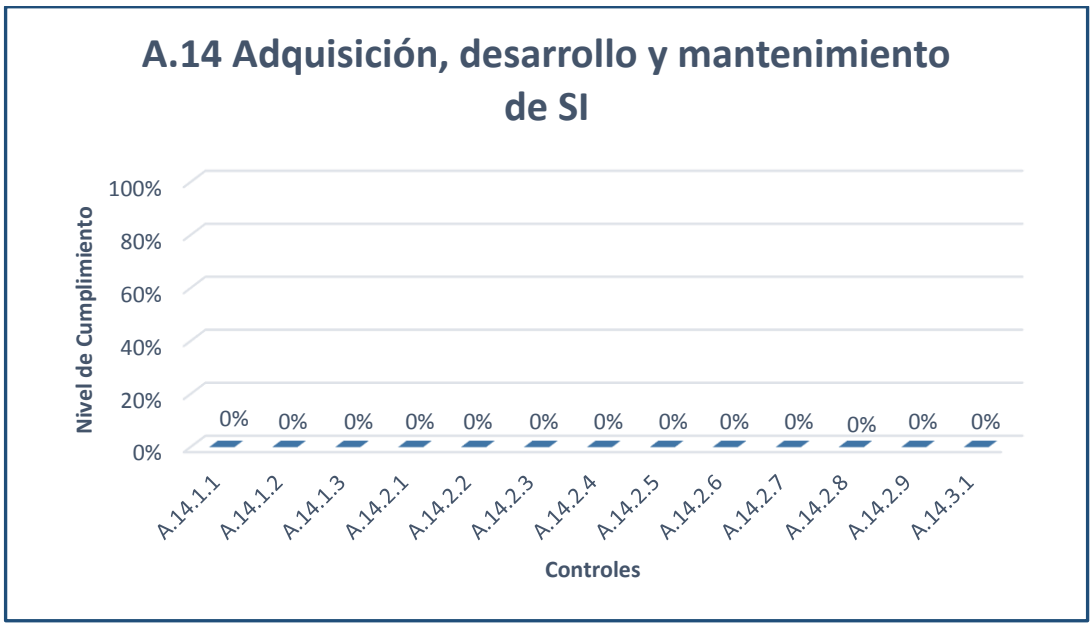
Cuadro 20. Controles seguridad de las comunicaciones

Controles	
A.13.1.1	Controles de redes
A.13.1.2	Seguridad de los servicios de red
A.13.1.3	Separación en las redes
A.13.2.1	Políticas y procedimientos de transferencia de información
A.13.2.2	Acuerdos sobre transferencia de información
A.13.2.3	Mensajería electrónica
A.13.2.4	Acuerdos de confidencialidad o de no divulgación
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.	

A.14 Adquisición, desarrollo y mantenimiento del SI: En la empresa Acceso Directo Asociados Limitada, no se tienen definidos requisitos de seguridad que se deben cumplir en cuanto a la adquisición de nuevo software o la actualización de software o aplicaciones existentes, en lo referente al uso de redes públicas no se ha definido ningún tipo de control guiado a mitigar fuga de información o acciones fraudulentas.

En cuanto a la seguridad en procesos de desarrollo y soporte, la empresa Acceso Directo Asociados Limitada, no hace ningún tipo de desarrollo propietario, todo software que se usa en la empresa es desarrollado por casas desarrolladoras.

Gráfica 20. Numeral A.14 anexo A norma ISO 27001:2013



Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.

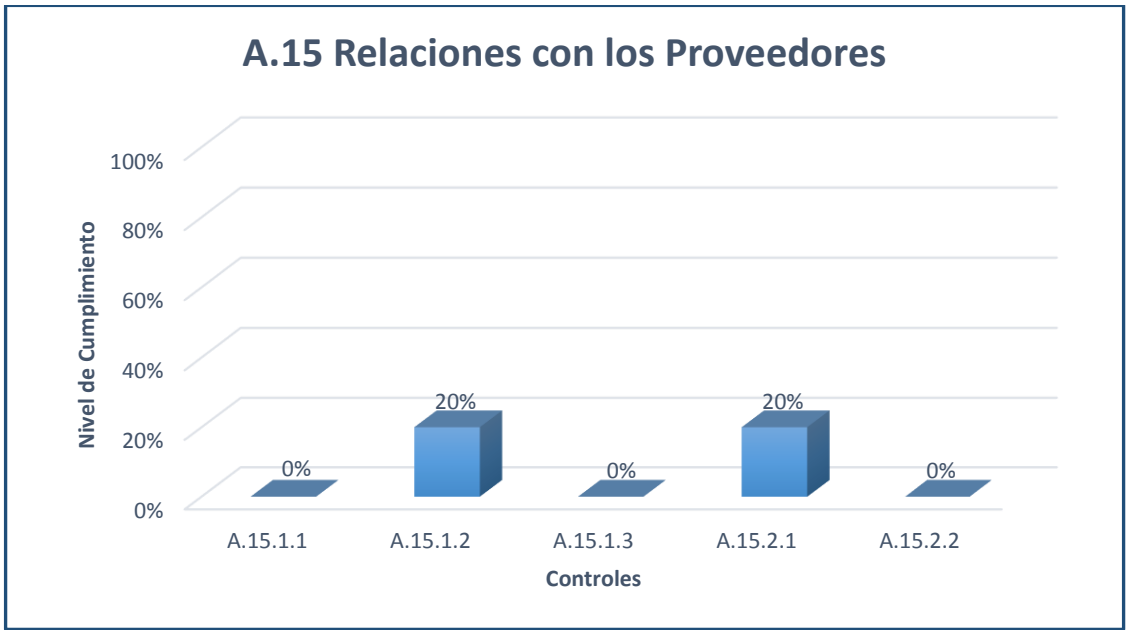
Cuadro 21. Controles de adquisición, desarrollo y mantenimiento SI

Controles	
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones
A.14.2.1	Política de desarrollo seguro
A.14.2.2	Procedimientos de control de cambios en sistemas
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación
A.14.2.4	Restricciones en los cambios a los paquetes de software
A.14.2.5	Principios de construcción de sistemas seguros
A.14.2.6	Ambiente de desarrollo seguro
A.14.2.7	Desarrollo contratado externamente
A.14.2.8	Pruebas de seguridad de sistemas
A.14.2.9	Prueba de aceptación de sistemas
A.14.3.1	Protección de datos de prueba
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.	

A.15 Relaciones con los proveedores: No hay políticas documentadas en cuanto a los requisitos de seguridad de la información que deben ser tomados en cuenta para mitigar los riesgos asociados con el acceso de proveedores a los activos, los proveedores no tienen acceso a la información, en caso de ser necesario no hay definido ningún proceso ni acuerdo de confidencialidad.

En cuanto a las auditorías se aplican algunos procesos, sin embargo, ninguno de estos procesos está documentado, ni existe alguna política definida para esto.

Gráfica 21. Numeral A.15 anexo A norma ISO 27001:2013.



Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.

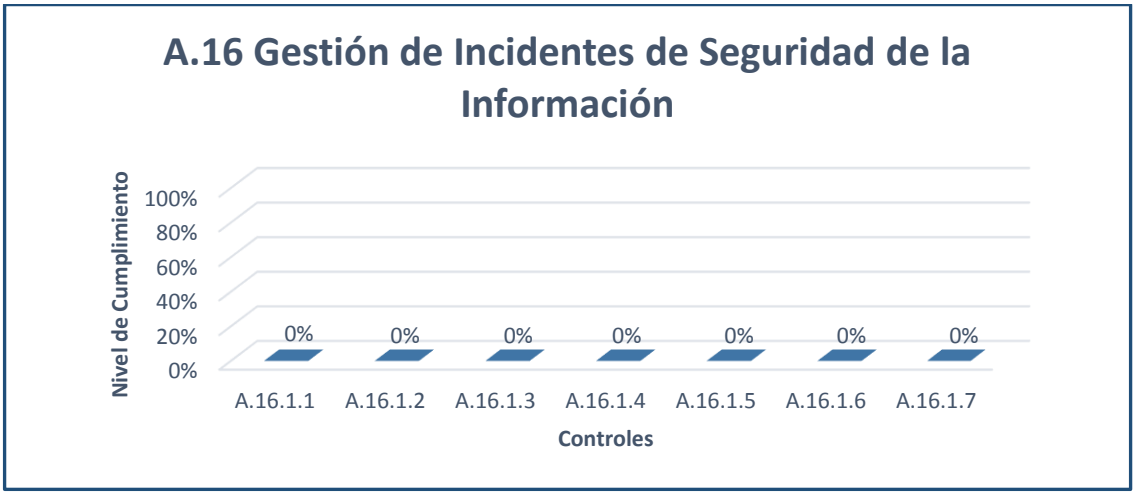
Cuadro 22. Controles relaciones con los proveedores

Controles	
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores
A.15.1.3	Cadena de suministro de tecnología de información y comunicación
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores
A.15.2.2	Gestión de cambios en los servicios de los proveedores
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.	

A.16 Gestión de Incidentes de Seguridad de la Información: Hoy en día no se han presentado incidentes que puedan poner en riesgo los objetivos de la empresa, la confidencialidad, integridad o disponibilidad de la información, no se tiene definida una política ni un CSIRT “Equipo de Respuesta a Incidentes de Seguridad Informática” que permita detectar, reportar, catalogar, dar tratamiento, recolectar y salvaguardar evidencia de posibles incidentes, para los funcionarios

de Acceso Directo Asociados Limitada no es una responsabilidad informar sobre la presencia de posibles incidentes de seguridad de la información.

Gráfica 22. Numeral A.16 anexo A norma ISO 27001:2013.



Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.

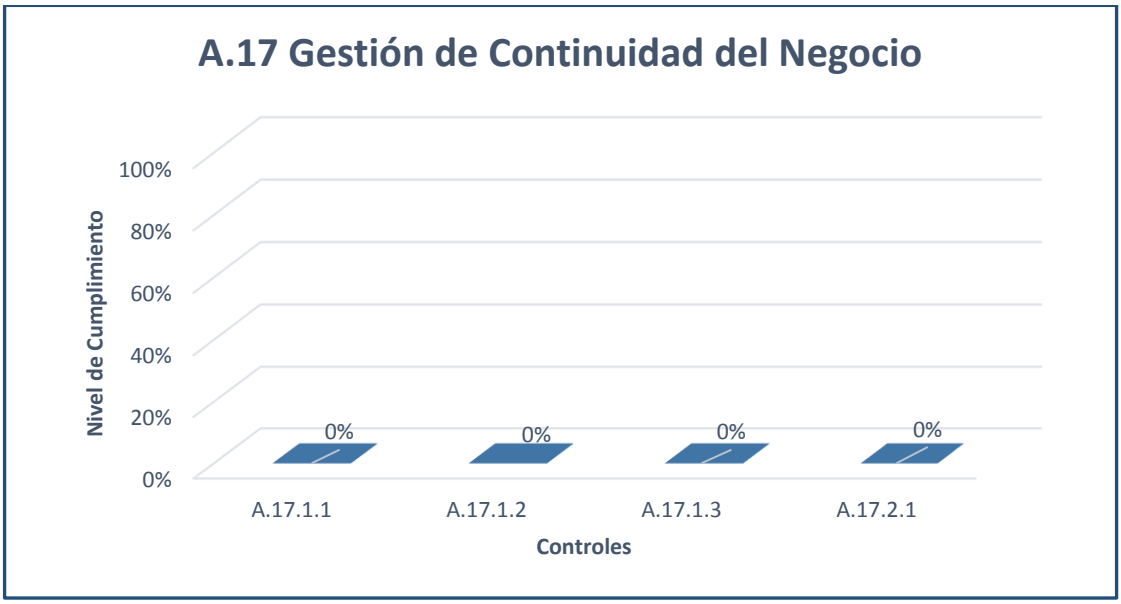
Cuadro 23. Controles gestión de incidentes de seguridad de la información

Controles	
A.16.1.1	Responsabilidades y procedimientos
A.16.1.2	Reporte de eventos de seguridad de la información
A.16.1.3	Reporte de debilidades de seguridad de la información
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos
A.16.1.5	Respuesta a incidentes de seguridad de la información
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información
A.16.1.7	Recolección de evidencia
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.	

A.17 Gestión de continuidad del negocio: Continuidad de seguridad de la Información. En caso de que un evento no permita desarrollar la operación normal de Acceso Directo Asociados Limitada en sus instalaciones físicas, no se ha establecido un plan para poder continuar con la operación de la empresa.

No se ha definido un documento donde se especifique las contingencias o el protocolo para la activación o continuidad de la operación normal de toda la empresa.

Gráfica 23. Numeral A.17 anexo A norma ISO 27001:2013



Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.

Cuadro 24. Controles gestión de continuidad del negocio

Controles	
A.17.1.1	Planificación de la continuidad de la seguridad de la información
A.17.1.2	Implementación de la continuidad de la seguridad de la información
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.	

A.18 Cumplimiento: Cumplimiento de requisitos legales y contractuales: Acceso Directo Asociados Limitada respecto a la seguridad de la información no se encuentra regulada por una entidad específica.

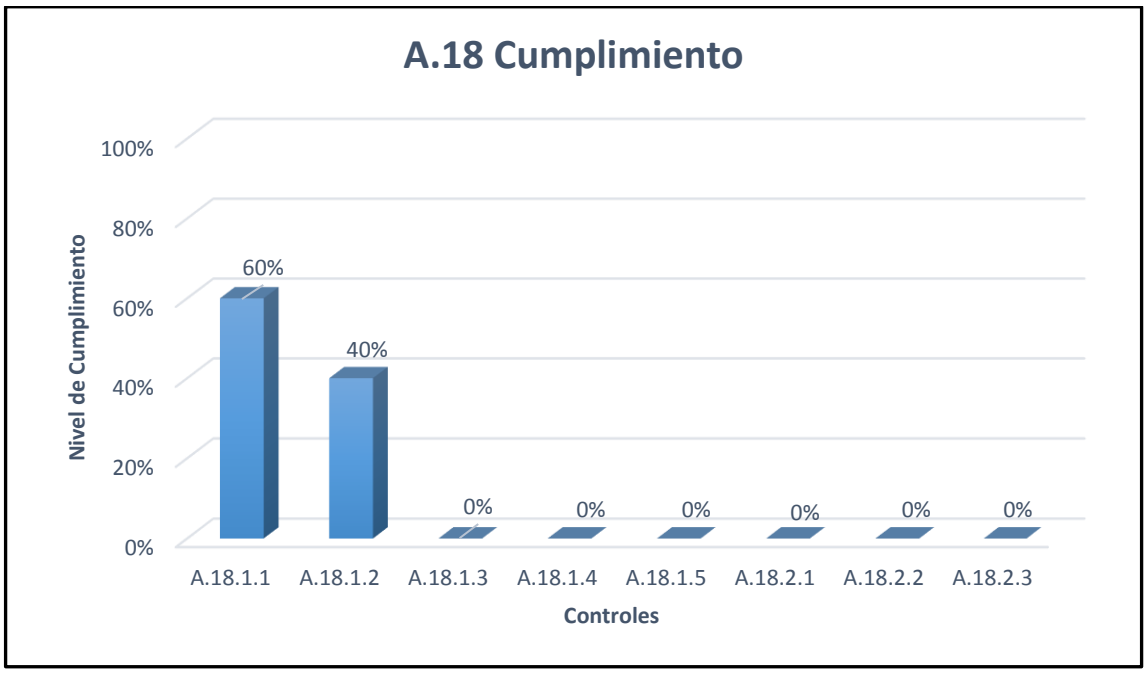
Por parte de la gerencia no tiene definida una política en la que se establezcan los mecanismos para proteger la información de clientes o propia respecto a pérdida,

destrucción, falsificación, acceso no autorizado y divulgación no autorizada, respecto a la protección de la información personal esta información personal de los funcionarios, esta es almacenada sin ninguna protección en la misma empresa.

Revisiones de Seguridad de la Información; nunca se han llevado a cabo revisiones las cuales tienen como objetivo establecer la definición de políticas de seguridad, su cumplimiento y como se logran los objetivos de la organización en cuanto a la seguridad de la información.

Es necesario tener en cuenta que la gerencia no ha establecido políticas y procedimientos, por ende, estos no pueden revisarse y actualizarse de acuerdo a las necesidades de seguridad de la información.

Gráfica 24. Numeral A.18 anexo A norma ISO 27001:2013.



Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.

Cuadro 25. Controles de cumplimiento

Controles	
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales
A.18.1.2	Derechos de propiedad intelectual
A.18.1.3	Protección de registros
A.18.1.4	Privacidad y protección de información de datos personales
A.18.1.5	Reglamentación de controles criptográficos
A.18.2.1	Revisión independiente de la seguridad de la información
A.18.2.2	Cumplimiento con las políticas y normas de seguridad
A.18.2.3	Revisión del cumplimiento técnico
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.	

6.2.3 Conclusiones del análisis GAP. La empresa Acceso Directo Asociados Limitada, contempla la seguridad de la información como una necesidad inmediata, han llevado a cabo procesos y procedimientos en su mayoría comunicados verbalmente e intentan definir roles y responsabilidades de seguridad informática en una sola persona, la misma que se encarga del área de sistemas, sin embargo, estos esfuerzos solo cubren algunos apartes de necesidades identificadas, pero no hacen parte de un proceso integral de seguridad de la información.

Se identifica la necesidad de la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) y definir políticas que permitan proteger la información, los activos de la empresa y dar cumplimiento a las normas vigentes.

Acceso Directo Asociados Limitada, necesita el diseño del Sistema de Gestión de Seguridad (SGSI), como los lineamientos a seguir para proteger de manera adecuada el core del negocio que para este caso son las campañas publicitarias desarrolladas dentro de la empresa, es indispensable garantizar la confidencialidad de los activos de información para generar seguridad en nuevos posibles clientes potenciales.

El alcance del sistema de gestión de seguridad de la información para la empresa Acceso Directo Asociados Limitada, está planteado para los procesos de gestión de información, gestión de recursos físicos y gestión humana.

Protección adecuada de la información: Con base en los resultados obtenidos del análisis GAP, se evidencia la necesidad de realizar un levantamiento de activos de información relevantes y de importancia vital para la empresa Acceso Directo Asociados Limitada, tomando como información principal el inventario de activos, realizando una matriz de riesgos, donde se identifiquen las principales amenazas y las vulnerabilidades a las que se puede ver expuesta la información calificada como crítica o confidencial, al tener el resultado de esta matriz de riesgos, realizar el levantamiento de un cuadro de controles tomando como referencia la Norma ISO 27001:2013.

6.3 RECOLECCIÓN DE ACTIVOS DE INFORMACIÓN

A continuación, se presenta la recolección de la información según la norma establecida.

6.3.1 Inventario de activos. La norma ISO27001 nos dice que todos los activos de información deben ser identificados de una forma clara y se tiene que realizar y mantener un inventario en el que aparezcan todos los activos de información importantes. Una empresa tiene que tener identificados todos sus activos y documentados en función de su importancia. El inventario de activos tiene que incluir toda la información que resulte necesaria con el fin de recuperarse ante un desastre, en la que se debe incluir el tipo de activo, el formato, la ubicación, la información de respaldo, la información de licencia y el valor de negocio. Los responsables de los activos y la clasificación de la información. Todo el proceso para crear el inventario de activos es un aspecto muy importante a la hora de gestionar los riesgos de la organización implementando un Sistema de Gestión de Seguridad de la Información ISO-27001. Una empresa tiene que identificar sus activos y el valor relativo de éstos[20]. Para realizar el inventario de activos de información en Acceso Directo Asociados Limitada, se realizó entrevista con uno de los dueños y la gerente de la empresa, también se tuvo en cuenta el material entregado por la empresa correspondiente al inventario de activos fijos que posee la empresa Acceso Directo Asociados Limitada.

[20] SGSI Blog especializado en Sistemas de Gestión . (18 de Febrero de 2017). Obtenido de SGSI Blog especializado en Sistemas de Gestión : http://www.pmg-ssi.com/2015/05/como-clasificar-los-activos-de-seguridad-en-un-sgsi/

Cuadro 26. Inventario de activos

Ítem No.	Nombre del activo	Proceso / Grupo	Tipo de activo de información	Cargo responsable
1	Impresoras	Sistemas	Hardware	Jefe oficina de Sistemas
2	Servidor de Información	Sistemas	Hardware	Jefe oficina de Sistemas
3	Computadores de escritorio	Sistemas	Hardware	Jefe oficina de Sistemas
4	Computadores portátiles	Sistemas	Hardware	Jefe oficina de Sistemas
5	Computadores de diseño (Apple)	Sistemas	Hardware	Jefe oficina de Sistemas
6	Discos duros externos	Sistemas	Hardware	Jefe oficina de Sistemas
7	Disco Duro Backups	Sistemas	Hardware	Jefe oficina de Sistemas
8	Consola de sonido	Diseño y publicidad	Hardware	Oficina de Diseño
9	Quemadores DVD	Diseño y publicidad	Hardware	Oficina de Diseño
10	Equipos DVD	Diseño y publicidad	Hardware	Oficina de Diseño
11	VHS	Diseño y publicidad	Hardware	Oficina de Diseño
12	Televisores	Gerencia	Hardware	Gerente
13	Microondas	Gerencia	Hardware	Gerente
14	Scanner	Sistemas	Hardware	Jefe oficina de Sistemas
15	Grabadoras Periodísticas	Diseño y publicidad	Hardware	Oficina de Diseño
16	Audífonos	Diseño y publicidad	Hardware	Oficina de Diseño
17	Tablet	Gerencia	Hardware	Gerente
18	Micrófonos	Diseño y publicidad	Hardware	Oficina de Diseño
19	Cámaras de Video	Diseño y publicidad	Hardware	Oficina de Diseño
20	Carros	Gerencia	Hardware	Gerente

Cuadro 26. (Continuación)

Ítem No.	Nombre del Activo	Proceso / Grupo	Tipo de Activo de Información	Cargo responsable
21	Contratos de servicio	Gerencia	Información	Gerente
22	Facturas	Oficina Financiera	Información	Contador
23	Servicios de Garantía	Gerencia	Información	Gerente
24	Órdenes de Compra	Oficina Financiera	Información	Contador
25	Ventas	Gerencia	Información	Gerente
26	Pago a proveedores	Oficina Financiera	Información	Contador
27	Nomina	Oficina Financiera	Información	Contador
28	Estados financieros	Oficina Financiera	Información	Contador
29	Empleados	Gestión Humana	Conocimiento	Encargado de gestión humana
30	Persona de mensajería	Gestión Humana	Conocimiento	Encargado de gestión humana
31	Diseñadores y publicistas	Gestión Humana	Conocimiento	Encargado de gestión humana
32	Servicio de Internet	Sistemas	Red	Jefe oficina de Sistemas
33	Servicio de Telefonía	Sistemas	Red	Jefe oficina de Sistemas
34	Red de datos	Sistemas	Red	Jefe oficina de Sistemas
35	Servicio de correo electrónico	Sistemas	Red	Jefe oficina de Sistemas
36	Circuito regulado	Sistemas	Red	Jefe oficina de Sistemas

Cuadro 26. (Continuación)

Ítem No.	Nombre del Activo	Proceso / Grupo	Tipo de Activo de Información	Cargo responsable
37	Suite de office	Sistemas	Software	Jefe oficina de Sistemas
38	Programas de diseño	Diseño y publicidad	Software	Oficina de Diseño
39	Programas de Edición	Diseño y publicidad	Software	Oficina de Diseño
40	Bases de datos de proveedores	Sistemas	Software	Jefe oficina de Sistemas
41	Antivirus	Sistemas	Software	Jefe oficina de Sistemas
42	Página Web	Sistemas	Software	Jefe oficina de Sistemas
43	Licencias software de diseño	Sistemas	Software	Jefe oficina de Sistemas
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.				

6.4 ANÁLISIS DE RIESGO

El análisis del riesgo implica el conocimiento del riesgo, este análisis ofrece una entrada para la evaluación del riesgo, y para decidir si es necesario o no tratar los riesgos y así mismo para definir los controles más adecuados para su respectivo tratamiento. El análisis de riesgo también ayuda para identificar los diferentes niveles de riesgo.

El análisis de riesgo implica la atención a las causas y las fuentes de los riesgos, sus consecuencias positivas y negativas, la probabilidad de que dichas consecuencias puedan ocurrir.

En esta etapa se realiza el análisis de los riesgos identificados con el fin de determinar el impacto de los mismos y se le asigna a cada uno de ellos un valor. En este caso puntual los valores asignados son: Muy Baja, Baja, Media, Alta y Muy Alta, como se muestra en el Cuadro 27. Valores de calificación matriz de riesgos.

Cuadro 27. Valores de calificación matriz de riesgos

Riesgo	Valores de calificación
Muy baja	1
Baja	2
Media	3
Alta	4
Muy Alta	5
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.	

El impacto que puede provocar la afectación de un activo de información se valoró de acuerdo a 4 aspectos los cuales son financiero, imagen, legal y continuidad operativa. En el Cuadro 28. Aspectos de valoración de impacto., se puede apreciar la valoración de impacto y la descripción de cada valor.

Cuadro 28. Aspectos de valoración de impacto.

Descriptor	Nivel	Financiero	Imagen	Legal	Continuidad operativa
		La pérdida de ingresos directa y los costos u otros gastos financieros indirectos que se generarían para la Empresa.	Afectación sobre la imagen y reputación de la Empresa.	Emisión de resoluciones administrativas y/o judiciales por el incumplimiento de normas, regulaciones u obligaciones.	Tiempo en que se ve afectada la operación de los procesos de la Empresa.
Insignificante	**1**	No se tendría consecuencias económicas que impacten el funcionamiento, por tanto, se asumirán las perdidas.	Grupo de funcionarios	Multas	Ajustes a una actividad concreta
Menor	**2**	Se tendría bajas consecuencias económicas.	Todos los funcionarios	Demandas	Cambios en los procedimientos
Moderado	**3**	Se tendría medianas consecuencias económicas.	Usuarios ciudad	Investigación Disciplinaria	Cambios en la interacción de los procesos
Mayor	**4**	Se tendría altas consecuencias económicas.	Usuarios Región	Investigación Fiscal	Intermitencia en el servicio
Catastrófico	**5**	Se tendría nefastas consecuencias económicas.	Usuarios País	Intervención - Sanción	Paro total del proceso
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.					

Para evaluar los riesgos fue necesario establecer la probabilidad de ocurrencia de los mismos, dado que el riesgo es el resultado de la operación entre el valor del impacto para la empresa si un activo es afectado contra la probabilidad de ocurrencia, se estableció la probabilidad de ocurrencia de acuerdo a la escala mostrada en el Cuadro 29. Probabilidad de ocurrencia., se evalúa con los siguientes niveles de probabilidad: raro, improbable, moderada, posible y casi certeza.

Cuadro 29. Probabilidad de ocurrencia.

Nivel de probabilidad		Descripción
1	**RARO**	El evento puede ocurrir solo en circunstancias excepcionales.
2	**IMPROBABLE**	El evento puede ocurrir en algún momento.
3	**MODERADA**	El evento podría ocurrir en algún momento.
4	**POSIBLE**	El evento probablemente ocurrirá en la mayoría de las circunstancias.
5	**CASI CERTEZA**	Se espera que el evento ocurra en la mayoría de las circunstancias.
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.		

Una vez identificados lo riesgos en la empresa se definió niveles del riesgo, para lo cual se diseñó una matriz de factores de tolerancia y respuesta a riegos. La cual se puede observar en el Cuadro 30. Matriz de factores de tolerancia y respuesta a riesgos.

Cuadro 30. Matriz de factores de tolerancia y respuesta a riesgos.

Límite Inferior	Límite Superior	Niveles de riesgo	Respuesta a los riesgos
3	53	BAJA	**Asumir el riesgo**
54	143	MODERADA	**Mitigar el riesgo, Evitar, Compartir**
144	279	ALTA	**Mitigar el riesgo, Evitar, Compartir**
280	375	EXTREMA	**Mitigar el riesgo, Evitar, Compartir**
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.			

Una vez identificados y analizados los riesgos, así como el impacto que tienen para el buen desempeño de la empresa se puede realizar el plan de tratamiento

de los riesgos basándose en los controles de la norma ISO 27001 que aplican para los riesgos identificados en Acceso Directo Asociados Limitada.

El plan de tratamiento de riesgos se fundamenta en establecer los controles necesarios para tratar los riesgos identificados.

6.4.1 Evaluación de riesgo. El propósito de la evaluación de riesgo es facilitar la toma de decisiones, basado en los resultados de dicho análisis, acerca de cuáles riesgos necesitan tratamiento con prioridad.

Los riesgos identificados se evaluarán de acuerdo a su nivel de probabilidad y de acuerdo al criterio de impacto sobre la seguridad de la información.

Se realizó la valoración de impacto para la empresa y probabilidad que un activo de información sea afectado por una amenaza.

En total se encontraron 7 riesgos en nivel baja, 26 moderados, 7 alta y 2 extrema, lo cual se puede evidenciar en el Cuadro 31. Resultado de evaluación del riesgo.

Cuadro 31. Resultado de evaluación del riesgo.

Límite inferior	Límite superior	Niveles de riesgo	Cantidad riesgos
3	53	BAJA	7
54	143	MODERADA	26
144	279	ALTA	7
280	375	EXTREMA	2
Fuente: Autores, según resultado revisión Acceso Directo Asociados Limitada.			

6.4.2 Lista de riesgos priorizados. Esta es la lista de los riesgos con mayor impacto y probabilidad de ocurrencia en la empresa y sobre los cuales la empresa debe mitigar y evitar para así no tener impactos perjudiciales:

- Falla en el sistema de copias de seguridad debido a que se almacenan en cintas guardadas en cajas sin ningún control de seguridad, los cuales son

vulnerables a la humedad y daños físicos, afectando la integridad de la información.

- Hurto o pérdida del disco duro de Backup por falta de control o copia no controlada.

- Mala manipulación de la información de nómina de pagos por falta de controles y verificación.

- Falla en la prestación de servicios u operación por ausencia de planes de continuidad de negocio.

- Ingeniería social en el personal de la compañía por falta de capacitación y concientización en seguridad de la información.

- Exposición indebida de información debido a la ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería.

- No existen políticas que definan el buen uso de los sistemas de información que se manejan en Acceso Directo Asociados Limitada, un funcionario o proveedor accidental o deliberadamente puede hacer mal uso de los mismos, sin que haya consecuencias.

- La disposición física de las carpetas, así como el uso y traslados necesarios para la ejecución de las labores, expone la información ante personas no autorizadas para tener conocimiento sobre el mismo o a condiciones ambientales o humanas que lleven a una eventual pérdida de la información.

6.4.3 Importancia de un análisis de riesgo. Uno de los requisitos más importantes definidos en la Norma ISO 27001:2013 es la gestión del riesgo, más allá del cumplimiento de los requisitos, la finalidad del análisis de riesgos hecho en Acceso Directo Asociados Limitada, es poder llevar a cabo la identificación, análisis y gestión de los mismos, lo que lleve a mejorar la eficiencia de la empresa en cuanto a:

- Efectividad de controles respecto a los riesgos y/o identificación de riesgo residual.

- Conocimiento del nivel de exposición a los riesgos identificados.

- Clasificación, evaluación y jerarquización de los riesgos que puedan afectar la seguridad de la información.

- Definición de planes de tratamiento para la administración de riesgos y de incidentes llegado el caso.

El análisis de riesgos se realiza con base a la norma ISO 27001:2013 en el apartado de planificación donde se aporta información que permite tomar decisiones en este caso particular por parte de la gerencia de la entidad sobre las acciones que se van a llevar a cabo para proteger los activos y la información de la empresa.

La gestión de riesgos puede ser llevada a cabo con metodologías propias de cada empresa siempre y cuando dichas metodologías garanticen los resultados, en el caso particular de Acceso Directo Asociados Limitada, para llevar a cabo el diseño del SGSI se hará uso de la metodología descrita en el estándar ISO27001:2013.

La fase de identificación de riesgos, dará como resultado la identificación de los riesgos a los que está expuesta la información y los activos de la empresa, tal como se encuentra funcionando en este momento, identificando el impacto de los mismos, se podrá llevar a cabo el análisis del riesgo y la valoración de los mismos.

6.4.4 Matriz de riesgos. Tomando como base el inventario de activos de información, se llevó a cabo la identificación de los activos principales en cada categoría identificando las vulnerabilidades y/o amenazas que se podrían explotar y los riesgos a los cuales están expuestos, dejando como resultado la matriz de riesgos de los activos de información primarios de la empresa Acceso Directo Asociados Limitada.

La matriz da resultados utilizando la teoría de la probabilidad de ocurrencia y el impacto generado en caso tal, es decir:

*Probabilidad de ocurrencia * impacto = riesgo*[21]

[21] Master en Gestión de Calidad y Reingenieria de Procesos. (s.f.). Obtenido de Master en Gestión de Calidad y Reingenieria de Procesos: http://www.eoi.es/blogs/mcalidadon/2016/02/03/la-matriz-probabilidad-impacto/

Los niveles de impacto y las probabilidades de ocurrencia fueron calculadas con base a las entrevistas realizadas a la gerencia y los responsables de cada activo de información, se identificaron en total 42 activos de información relevante y de gran importancia para la empresa Acceso Directo Asociados Limitada.

Cuadro 32. Matriz de riesgos

Ítem no.	Nombre del activo	Proceso / grupo	Tipo de activo de información	Cargo responsable	Custodio	Medio de almacenamiento	Ubicación	Estado del activo	Propiedades de seguridad del activo de información						Valor del activo		Identificación vulnerabilidad y amenaza (causa)	Identificación del riesgo	Tipo de riesgo	Dueño del riesgo	Riesgo asociado a c-i-d	Tipo de impacto	Valor impacto	Nivel impacto	Valor probabilidad	Nivel probabilidad del riesgo	Valor riesgo	Nivel de riesgo
									Confidencialidad		Integridad		Disponibilidad															
									Nivel	Valor	Nivel	Valor	Nivel	Valor	Nivel	Valor												
1	Archivos de pago de nómina/Proveedores	Gestión Financiera	Información Pura	Directora de Talento Humano	Gerente Administrativo	Combinado	Oficina Administrativa	Activo	Media	3	Muy Alta	5	Alta	4	Alto	12	Los archivos de pago de nómina, a proveedores, se consolidan mediante un proceso manual (En Excel) en el cual intervienen varias personas, antes de guardar el archivo definitivo del pago de nómina a una Carpeta del equipo del Gerente Administrativo. Una persona podría cambiar accidental o intencionalmente el valor de los pagos que se debe realizar en Acceso Directo Asociados Limitada.	Pérdida de la integridad de la información	Físico	Coordinador del grupo de Nómina	Integridad	FINANCIERO	5	Catastrófico	5	Casi Certeza	300	**EXTREMA**
2	Historias clínicas	Gestión Humana	Información Pura	Director Gestión del Talento Humano	Director Gestión del Talento Humano	Físico	Oficina Administrativa	Activo	Muy Alta	5	Muy Alta	5	Muy Alta	5	Muy Alto	15	Este archivo presenta un alto grado de confidencialidad por lo que se requiere exclusividad de almacenamiento	Pérdida de la disponibilidad de la información	Lógico	Director Gestión del Talento Humano	Confidencialidad	LEGAL	5	Catastrófico	5	Casi Certeza	375	**EXTREMA**
3	Archivo físico (expedientes y archivos de gestión)	Gestión de Información	Información Pura	Gerente Operativa	Gerente Operativa	Físico	Oficina Operativa	Activo	Media	3	Alta	4	Muy Alta	5	Alto	12	Las cámaras de baja definición o ausencia de las mismas disminuyen el control efectivo sobre la documentación.	Pérdida de la disponibilidad de la información Pérdida de la confidencialidad de la información	Físico	Gerente Administrativo	Confidencialidad - Integridad - Disponibilidad	CONTINUIDAD OPERATIVA	3	Moderado	5	Casi Certeza	180	ALTA
4	Base de Datos de contratos (Excel)	Gestión Humano	Información Pura	Gerente Administrativo	Gerente Administrativo	Combinado	Oficina Administrativa	Activo	Media	3	Muy Alta	5	Muy Alta	5	Muy Alto	13	El almacenamiento del archivo en formato editable, además de un almacenamiento compartido, hace la información susceptible a ser modificada	Pérdida de la integridad de la información	Lógico	Gerente Administrativo	Integridad	CONTINUIDAD OPERATIVA	4	Mayor	3	Moderada	156	ALTA

Cuadro 32. (Continuación)

Ítem No.	Nombre del Activo	Proceso / grupo	Tipo de activo de información	Cargo responsable	Custodio	Medio de almacenamiento	Ubicación	Estado del activo	Propiedades de seguridad del activo de información						Valor del activo		Identificación vulnerabilidad y amenaza (causa)	Identificación del riesgo	Tipo de riesgo	Dueño del riesgo	Riesgo asociado a c-i-d	Tipo de impacto	Valor impacto	Nivel impacto	Valor probabilidad	Nivel probabilidad del riesgo	Valor riesgo	Nivel de riesgo
									Confidencialidad		Integridad		Disponibilidad															
									Nivel	Valor	Nivel	Valor	Nivel	Valor	Nivel	Valor												
5	Documentos de novedad del personal (incapacidad, vacaciones, licencias, certificaciones retención en la fuente, resoluciones de encargo, prima técnica, solicitudes de embargos)	Gestión Humano	Información Pura	Subdirectora de Talento Humano	Oficina Administrativa	Digital	Oficina Administrativa	Activo	Media	3	Muy Alta	5	Alta	4	Alto	12	Documentos de novedad del personal se almacenan en una carpeta compartida sin permisos definidos. Una persona podría cambiar o borrar accidental o intencionalmente el contenido de dicha carpeta	Pérdida de la integridad y disponibilidad de la información	Lógico	Coordinador del grupo de Nómina / Jefe Sistemas	Integridad - Disponibilidad	CONTINUIDAD OPERATIVA	4	Mayor	3	Moderada	144	ALTA
6	Cintas magnéticas	Gestión de Recursos Físicos	Información Pura	Jefe de Sistemas	Jefe de Sistemas	Digital	Oficina de Sistemas - Soporte Informático	Activo	Alta	4	Alta	4	Muy Alta	5	Muy Alto	13	Los Backups, se almacenan en cintas guardadas en cajas sin ningún control de seguridad, los cuales son vulnerables a la humedad y daños físicos, afectando la integridad de la información.	Pérdida de la integridad de la información.	Físico	Jefe de Sistemas	Integridad	CONTINUIDAD OPERATIVA	4	Mayor	4	Posible	208	ALTA
7	Informe de depuración de datos	Gestión de Información	Información Pura	Secretario General de la Empresa	Secretario General de la Empresa	Digital	Oficina de Sistemas - Soporte Informático	Activo	Media	3	Media	3	Media	3	Medio	9	No existen políticas que definan el buen uso de los sistemas de información que se manejan en Acceso Directo Asociados Limitada, Un Funcionario o proveedor accidental o deliberadamente puede hacer mal uso de los mismos, sin que haya consecuencias.	pérdida de imputabilidad	Legal	Gerente Administrativo	Confidencialidad - Integridad - Disponibilidad	LEGAL	4	Mayor	5	Casi Certeza	180	ALTA
8	Carpetas Historias Laborales	Gestión Humano	Información Pura	Director Gestión del Talento Humano	Director Gestión del Talento Humano	Combinado	Oficina Administrativa	Activo	Baja	2	Media	3	Media	3	Medio	8	La disposición física de las carpetas físicas, así como el uso y traslados necesarios para la ejecución de las labores, expone la información ante personas no autorizadas para tener conocimiento sobre el mismo o a condiciones ambientales o humanas que lleven a una eventual pérdida de la información.	Pérdida de la disponibilidad, integridad y/o confidencialidad de la información.	Legal	Director Gestión del Talento Humano	Integridad	LEGAL	5	Catastrófico	4	Posible	160	ALTA
9	Archivo de seguridad y salud en el trabajo	Gestión Humana	Información Pura	Director Gestión del Talento Humano	Gestión del Talento Humano	Físico	Oficina Administrativa	Activo	Muy Alta	5	Muy Alta	5	Muy Alta	5	Muy Alto	15	Este archivo presenta un alto grado de confidencialidad por lo que se requiere exclusividad de almacenamiento	Pérdida de la confidencialidad de la información	Lógico	Director Gestión del Talento Humano	Confidencialidad	LEGAL	5	Catastrófico	3	Moderada	225	ALTA

Cuadro 32. (Continuación)

Ítem No.	Nombre del Activo	Proceso / Grupo	Tipo de Activo de información	Cargo Responsable	Custodio	Medio de almacenamiento	Ubicación	Estado del Activo	Propiedades de seguridad del activo de información						Valor del activo		Identificación vulnerabilidad y amenaza (causa)	Identificación del riesgo	Tipo de riesgo	Dueño del riesgo	Riesgo asociado a c-i-d	Tipo de impacto	Valor impacto	Nivel impacto	Valor probabilidad	Nivel probabilidad del riesgo	Valor riesgo	Nivel de riesgo
									Confidencialidad		Integridad		Disponibilidad															
									Nivel	Valor	Nivel	Valor	Nivel	Valor	Nivel	Valor												
10	Libro de ingreso de personas a Acceso Directo Asociados Limitada	Gestión Humana	Información Pura	Secretario General de la Empresa	Secretario General de la Empresa	Físico	Oficina Administrativa	Activo	Alta	4	Alta	4	Media	3	Alto	11	Base de datos de ingreso de personas a la empresa, se almacena en un medio físico susceptible a las condiciones ambientales y errores en su manipulación. (Libro)	Pérdida de la integridad y disponibilidad de la información	Físico	Secretario General	Integridad - Disponibilidad	CONTINUIDAD OPERATIVA	2	Menor	4	Posible	88	MODERADA
11	Base de datos de registro y seguimiento de servicios	Gestión Humana	Información Pura	Secretario General de la Empresa	Secretario General de la Empresa	Digital	Oficina Administrativa	Activo	Media	3	Alta	4	Baja	2	Medio	9	La base de datos del registro y seguimiento de servicios, se gestiona desde un archivo plano en Excel, sin protección contra lectura, escritura o eliminación de la información	pérdida de la confidencialidad, integridad y/o disponibilidad de la información	Lógico	Secretario General	Confidencialidad - Integridad - Disponibilidad	CONTINUIDAD OPERATIVA	3	Moderado	2	Improbable	54	MODERADA
12	Equipos de Audiovisuales	Gestión de Recursos Físicos	Hardware	Jefe de Sistemas	Jefe de Sistemas	Físico	Oficina de Sistemas - Soporte Informático	Activo	Media	3	Media	3	Muy Alta	5	Alto	11	Acceso directo Asociados Limitada, no ha implementado controles, difundido los procedimientos y políticas de seguridad de la información. Hay un desconocimiento general, lo cual implica divulgación o modificación o eliminación no autorizada de la información.	Pérdida de la integridad y disponibilidad de la información	Físico	Jefe de Sistemas	Confidencialidad - Integridad - Disponibilidad	CONTINUIDAD OPERATIVA	3	Moderado	3	Moderada	99	MODERADA
13	Informe de encuesta de satisfacción	Gestión Humano	Información Pura	Comunicadoras Sociales o Ejecutivo de Cuenta	Atención al ciudadano	Físico	Oficina Operativa	Activo	Muy Baja	1	Media	3	Baja	2	Bajo	6	Todos los informes se envían por medio del correo electrónico, sin embargo, no existen mecanismos para determinar la autenticación de origen y el no repudio. Un atacante podría suplantar la identidad del propietario de la información.	Pérdida de la autenticación de origen de la información	Reputación	Jefe de Sistemas	Integridad	IMAGEN	5	Catastrófico	2	Improbable	60	MODERADA
14	Información Contractual	Gestión de Información	Información Pura	Secretario General de la Empresa	Secretario General de la Empresa	Combinado	Oficina Administrativa	Activo	Alta	4	Media	3	Muy Alta	5	Alto	12	Todos los informes se envían por medio del correo electrónico, sin embargo, no existen mecanismos para determinar la autenticación de origen y el no repudio. Un atacante podría suplantar la identidad del propietario de la información.	Pérdida de la integridad de la información	Legal	Jefe de Sistemas	Integridad	LEGAL	5	Catastrófico	2	Improbable	120	MODERADA
15	Información de Saneamiento de bienes, muebles e inmuebles	Gestión de Recursos Físicos	Información Pura	Secretario General de la Empresa	Jefe de Sistemas	Combinado	Oficina Administrativa	Activo	Media	3	Media	3	Muy Alta	5	Alto	11	Todos los informes se envían por medio del correo electrónico, sin embargo, no existen mecanismos para determinar la autenticación de origen y el no repudio. Un atacante podría suplantar la identidad del propietario de la información.	Pérdida de la integridad de la información	Legal	Jefe Sistemas	Integridad	LEGAL	3	Moderado	2	Improbable	66	MODERADA

Cuadro 32. (Continuación)

Ítem No.	Nombre del Activo	Proceso / Grupo	Tipo de Activo de información	Cargo Responsable	Custodio	Medio de almacenamiento	Ubicación	Estado del Activo	Propiedades de seguridad del activo de información						Valor del activo		Identificación vulnerabilidad y amenaza (causa)	Identificación del riesgo	Tipo de riesgo	Dueño del riesgo	Riesgo asociado a c-i-d	Tipo de impacto	Valor impacto	Nivel impacto	Valor probabilidad	Nivel probabilidad del riesgo	Valor riesgo	Nivel de riesgo
									Confidencialidad		Integridad		Disponibilidad															
									Nivel	Valor	Nivel	Valor	Nivel	Valor	Nivel	Valor												
16	Información de histórico de Equipos Audiovisuales e inmuebles	Gestión de Recursos Físicos	Información Pura	Secretario General de la Empresa	Jefe de Sistemas	Combinado	Oficina de Sistemas	Activo	Alta	4	Media	3	Muy Alta	5	Alto	12	Todos los informes se envían por medio del correo electrónico, sin embargo, no existen mecanismos para determinar la autenticación de origen y el no repudio. Un atacante podría suplantar la identidad del propietario de la información.	Pérdida de la integridad de la información	Lógico	Jefe de Sistemas	Integridad	CONTINUIDAD OPERATIVA	3	Moderado	2	Improbable	72	**MODERADA**
17	Base de datos de seguimiento de los procesos disciplinarios	Gestión de Información	Información Pura	Secretario General de la Empresa	Secretario General de la Empresa	Digital	Oficina Administrativa	Activo	Alta	4	Muy Alta	5	Muy Alta	5	Muy Alto	14	El almacenamiento de información en una estación de trabajo de uso operativo constante, sin una copia de respaldo adecuada, lo cual puede ocasionar pérdidas de información a causa de fallas en hardware o software en el equipo	Pérdida confidencialidad, integridad y disponibilidad de la información	Legal	Secretario General	Confidencialidad - Integridad - Disponibilidad	LEGAL	3	Moderado	3	Moderada	126	**MODERADA**
18	Base de Datos de contratos (Excel)	Gestión Humano	Información Pura	Gerente Administrativo	Gerente Administrativo	Combinado	Oficina Administrativa	Activo	Media	3	Muy Alta	5	Muy Alta	5	Muy Alto	13	El almacenamiento en una estación de trabajo de uso operativo constante sin una copia de respaldo adecuada puede ocasionar pérdidas de información a causa de fallas en hardware o software en el equipo	Pérdida de la disponibilidad de la información	Lógico	Gerente Administrativo	Disponibilidad	CONTINUIDAD OPERATIVA	3	Moderado	3	Moderada	117	**MODERADA**
19	Base de Datos de Procesos (Excel)	Gestión de Información	Información Pura	Secretario General de la Empresa	Secretario General de la Empresa	Digital	Oficina Administrativa	Activo	Media	3	Muy Alta	5	Muy Alta	5	Muy Alto	13	El almacenamiento del archivo en formato editable, además de un almacenamiento compartido, hace la información susceptible a ser modificada	Pérdida de la integridad de la información	Lógico	Secretario General	Integridad	CONTINUIDAD OPERATIVA	3	Moderado	3	Moderada	117	**MODERADA**
20	Hoja de vida de los funcionarios (Soportes)	Gestión Humana	Información Pura	Directora de Talento Humano	Gerente Administrativo	Combinado	Oficina Administrativa	Activo	Baja	2	Muy Alta	5	Alta	4	Alto	11	Las hojas de vida de los funcionarios, incluyendo sus soportes, no se radican por medio del proceso de Gestión Documental (Orfeo), lo cual podría implicar la Pérdida de la trazabilidad de los documentos o integridad de los mismos, principalmente en el caso puntual de los préstamos.	Pérdida de la integridad y disponibilidad de la información	Lógico	Secretario General	Integridad - Disponibilidad	LEGAL	4	Mayor	3	Moderada	132	**MODERADA**
21	Documentos soportes de verificación de requisitos	Gestión Humana	Información Pura	Directora de Talento Humano	Gerente Administrativo	Digital	Oficina Administrativa	Activo	Media	3	Muy Alta	5	Baja	2	Alto	10	Durante el trámite de verificación de requisitos, los documentos soporte son manipulados, como parte de su labor diaria, por varios funcionarios. Lo anterior, puede implicar la Pérdida de la trazabilidad de los documentos.	Pérdida de la trazabilidad de la información	Físico	Coordinador del grupo de Nómina / Director Talento Humano	Disponibilidad	CONTINUIDAD OPERATIVA	3	Moderado	2	Improbable	60	**MODERADA**

Cuadro 32. (Continuación)

Ítem No.	Nombre del Activo	Proceso / Grupo	Tipo de Activo de información	Cargo Responsable	Custodio	Medio de almacenamiento	Ubicación	Estado del Activo	Propiedades de seguridad del activo de información						Valor del activo		Identificación vulnerabilidad y amenaza (causa)	Identificación del riesgo	Tipo de riesgo	Dueño del riesgo	Riesgo asociado a c-i-d	Tipo de impacto	Valor impacto	Nivel impacto	Valor probabilidad	Nivel probabilidad del riesgo	Valor riesgo	Nivel de riesgo
									Confidencialidad		Integridad		Disponibilidad															
									Nivel	Valor	Nivel	Valor	Nivel	Valor	Nivel	Valor												
22	Resolución de vinculación/ Retiro	Gestión Humana	Información Pura	Directora de Talento Humano	Gerente Administrativo	Combinado	Carpeta Compartida	Activo	Muy Baja	1	Muy Alta	5	Alta	4	Alto	10	Acceso Directo Asociados Limitada, no ha implementado controles, difundido los procedimientos y políticas de seguridad de la información. hay un desconocimiento general, lo cual implica divulgación o modificación o eliminación no autorizada de la información	pérdida de la confidencialidad, integridad disponibilidad de la información	Lógico	Gerente Administrativo	Confidencialidad - Integridad - Disponibilidad	CONTINUIDAD OPERATIVA	3	Moderado	3	Moderada	90	**MODERADA**
23	Soportes de pre-liquidación (autocontrol)	Gestión Financiera	Información Pura	Gerente Administrativo	Oficina Administrativa	Digital	Oficina Administrativa	Activo	Media	3	Media	3	Muy Alta	5	Alto	11	Limitada, no ha implementado controles, difundido los procedimientos y políticas de seguridad de la información. hay un desconocimiento general, lo cual implica divulgación o modificación o eliminación no autorizada de la información	pérdida de la confidencialidad, integridad disponibilidad de la información	Lógico	Gerente Administrativo	Confidencialidad - Integridad - Disponibilidad	CONTINUIDAD OPERATIVA	3	Moderado	3	Moderada	99	**MODERADA**
24	Correos con soportes de trámite de la novedad	Gestión Financiera	Información Pura	Gerente Administrativo	Oficina Administrativa	Digital	Servidor Correo	Activo	Media	3	Media	3	Muy Alta	5	Alto	11	Acceso Directo Asociados Limitada, no ha implementado controles, difundido los procedimientos y políticas de seguridad de la información. hay un desconocimiento general, lo cual implica divulgación o modificación o eliminación no autorizada de la información	pérdida de la confidencialidad, integridad disponibilidad de la información	Lógico	Gerente Administrativo	Confidencialidad - Integridad - Disponibilidad	CONTINUIDAD OPERATIVA	3	Moderado	3	Moderada	99	**MODERADA**
25	Planillas de nómina, Aportes a seguridad social/Fondo nacional del ahorro/ Embargos	Gestión Financiera	Información Pura	Gerente Administrativo	Oficina Administrativa	Digital	Oficina Administrativa	Activo	Media	3	Muy Alta	5	Muy Alta	5	Muy Alto	13	Acceso Directo Asociados Limitada, no ha implementado controles, difundido los procedimientos y políticas de seguridad de la información. hay un desconocimiento general, lo cual implica divulgación o modificación o eliminación no autorizada de la información	pérdida de la confidencialidad, integridad disponibilidad de la información	Lógico	Gerente Administrativo	Confidencialidad - Integridad - Disponibilidad	CONTINUIDAD OPERATIVA	4	Mayor	2	Improbable	104	**MODERADA**
26	Recibo de nómina, ingreso y retenciones	Gestión Financiera	Información Pura	Gerente Administrativo	Oficina Administrativa	Digital	Oficina Administrativa	Activo	Baja	2	Muy Alta	5	Muy Alta	5	Alto	12	Acceso Directo Asociados Limitada, no ha implementado controles, difundido los procedimientos y políticas de seguridad de la información. hay un desconocimiento general, lo cual implica divulgación o modificación o eliminación no autorizada de la información	pérdida de la confidencialidad, integridad disponibilidad de la información	Lógico	Gerente Administrativo	Confidencialidad - Integridad - Disponibilidad	CONTINUIDAD OPERATIVA	3	Moderado	3	Moderada	108	**MODERADA**

Cuadro 32. (Continuación)

Ítem No.	Nombre del Activo	Proceso / Grupo	Tipo de Activo de información	Cargo Responsable	Custodio	Medio de almacenamiento	Ubicación	Estado del Activo	Propiedades de seguridad del activo de información						Valor del activo		Identificación vulnerabilidad y amenaza (causa)	Identificación del riesgo	Tipo de riesgo	Dueño del riesgo	Riesgo asociado a c-i-d	Tipo de impacto	Valor impacto	Nivel impacto	Valor probabilidad	Nivel probabilidad del riesgo	Valor riesgo	Nivel de riesgo
									Confidencialidad		Integridad		Disponibilidad															
									Nivel	Valor	Nivel	Valor	Nivel	Valor	Nivel	Valor												
27	Capacidad de endeudamiento	Gestión Financiera	Información Pura	Gerente Administrativo	Oficina Administrativa	Digital	Oficina Administrativa	Activo	Media	3	Muy Alta	5	Media	3	Alto	11	Acceso Directo Asociados Limitada, no ha implementado controles, difundido los procedimientos y políticas de seguridad de la información. hay un desconocimiento general, lo cual implica divulgación o modificación o eliminación no autorizada de la información	pérdida de la confidencialidad, integridad disponibilidad de la información	Lógico	Gerente Administrativo	Confidencialidad - Integridad - Disponibilidad	CONTINUIDAD OPERATIVA	3	Moderado	3	Moderada	99	**MODERADA**
28	Resolución de vacaciones, prestaciones pagadas	Gestión Financiera	Información Pura	Gerente Administrativo	Oficina Administrativa	Digital	Oficina Administrativa	Activo	Media	3	Muy Alta	5	Alta	4	Alto	12	Acceso Directo Asociados Limitada, no ha implementado controles, difundido los procedimientos y políticas de seguridad de la información. hay un desconocimiento general, lo cual implica divulgación o modificación o eliminación no autorizada de la información	pérdida de la confidencialidad, integridad disponibilidad de la información	Lógico	Gerente Administrativo	Confidencialidad - Integridad - Disponibilidad	CONTINUIDAD OPERATIVA	3	Moderado	3	Moderada	108	**MODERADA**
29	Información de infraestructura tecnológica (hardware/software)	Gestión de Información	Información Pura	Jefe de Sistemas	Jefe de Sistemas	Digital	Oficina de Sistemas - Soporte Informático	Activo	Alta	4	Media	3	Muy Alta	5	Alto	12	Acceso Directo Asociados Limitada, no ha implementado controles, difundido los procedimientos y políticas de seguridad de la información. hay un desconocimiento general, lo cual implica divulgación o modificación o eliminación no autorizada de la información	pérdida de la confidencialidad, integridad disponibilidad de la información	Lógico	Jefe de Sistemas	Confidencialidad - Integridad - Disponibilidad	CONTINUIDAD OPERATIVA	3	Moderado	3	Moderada	108	**MODERADA**
30	Cintas magnéticas.	Gestión de Recursos Físicos	Información Pura	Jefe de Sistemas	Jefe de Sistemas	Digital	Oficina de Sistemas - Soporte Informático	Activo	Alta	4	Alta	4	Muy Alta	5	Muy Alto	13	La información se ubica la oficina de Sistemas, la cual es de libre de acceso sin restricción, cualquier persona que ingrese a esta oficina puede tener acceso no autorizado a la información.	Pérdida de disponibilidad de información	Físico	Jefe de Sistemas	Disponibilidad	CONTINUIDAD OPERATIVA	3	Moderado	3	Moderada	117	**MODERADA**
31	Información de informes y Metodologías de versiones anteriores.	Gestión de Información	Información Pura	Secretario General de la Empresa	Secretario General de la Empresa	Digital	Oficina Administrativa	Activo	Alta	4	Muy Alta	5	Media	3	Alto	12	La información se almacena en un medio físico susceptible a las condiciones ambientales y errores en su manipulación (CD)	Pérdida de la integridad y disponibilidad de la información	Lógico	Gerente Administrativo	Integridad	CONTINUIDAD OPERATIVA	3	Moderado	3	Moderada	108	**MODERADA**

Cuadro 32. (Continuación)

Ítem No.	Nombre del Activo	Proceso / Grupo	Tipo de Activo de información	Cargo Responsable	Custodio	Medio de almacenamiento	Ubicación	Estado del Activo	Propiedades de seguridad del activo de información						Valor del activo		Identificación vulnerabilidad y amenaza (causa)	Identificación del riesgo	Tipo de riesgo	Dueño del riesgo	Riesgo asociado a c-i-d	Tipo de impacto	Valor impacto	Nivel impacto	Valor probabilidad	Nivel probabilidad del riesgo	Valor riesgo	Nivel de riesgo
									Confidencialidad		Integridad		Disponibilidad															
									Nivel	Valor	Nivel	Valor	Nivel	Valor	Nivel	Valor												
32	Información de procesos y procedimientos en proceso de publicación.	Gestión de Información	Información Pura	Ejecutivo de Cuenta	Ejecutivo de Cuenta	Digital	Oficina Operativa	Activo	Media	3	Media	3	Muy Alta	5	Alto	11	No se tiene toda la documentación técnica actualizada de los sistemas de información y la base de datos de Acceso Directo Asociados Limitada, por tal motivo genera demoras en el apoyo de desarrollo de procedimientos tecnológicos.	Reproceses	Lógico	Gerente Administrativo	Disponibilidad	CONTINUIDAD OPERATIVA	3	Moderado	3	Moderada	72	**MODERADA**
33	Procesos de trámites y servicios del Acceso Directo Asociados Limitada	Gestión Financiera	Información Pura	Ejecutivo de Cuenta	Ejecutivo de Cuenta	Digital	Oficina Operativa	Activo	Media	3	Alta	4	Baja	2	Medio	9	No se cuenta con una política de uso y privacidad que referencie a los Procesos de trámites y servicios que Acceso Directo Asociados Limitada ofrece desde su portal Web, de conformidad con la ley 1581 de 2012	Incumplimiento legal	Legal	Gerente Administrativo	Integridad	LEGAL	4	Mayor	3	Moderada	108	**MODERADA**
34	Portal Web de Acceso Directo Asociados Limitada	Gestión de Información	Software	Jefe de sistemas	Jefe de Sistemas	Digital	Oficina de Sistemas	Activo	Muy Baja	1	Muy Alta	5	Muy Alta	5	Alto	11	Acceso Directo Asociados Limitada, no ha implementado controles, difundido los procedimientos y políticas de seguridad de la información. hay un desconocimiento general, lo cual implica divulgación o modificación o eliminación no autorizada de la información	pérdida de la confidencialidad, integridad disponibilidad de la información	Lógico	Gerente Administrativo	Confidencialidad - Integridad - Disponibilidad	CONTINUIDAD OPERATIVA	3	Moderado	3	Moderada	99	**MODERADA**
35	Archivos de capacitación	Gestión Humana	Información Pura	Director Gestión del Talento Humano	Director Gestión del Talento Humano	Digital	Oficina Administrativa	Activo	Muy Baja	1	Alta	4	Alta	4	Medio	9	El archivo soporte de capacitaciones realizadas y el material necesario para capacitaciones futuras no cuenta con Backup, por lo que ante un eventual daño de equipo o falla en los archivos expone la información a una pérdida irrecuperable.	Pérdida de la disponibilidad de la información	Físico	Jefe de Sistemas	Disponibilidad	CONTINUIDAD OPERATIVA	2	Menor	3	Moderada	54	**MODERADA**
36	Planilla de entrega de correspondencia de salida	Gestión de Información	Información Pura	Secretario General de la Empresa	Secretario General de la Empresa	Físico	Archivo Central (Oficina Administrativa)	Activo	Media	3	Media	3	Baja	2	Medio	8	Acceso Directo Asociados Limitada, no ha implementado controles, difundido los procedimientos y políticas de seguridad de la información. hay un desconocimiento general, lo cual implica divulgación o modificación o eliminación no autorizada de la información	pérdida de la confidencialidad, integridad disponibilidad de la información	Lógico	Secretario General	Confidencialidad - Integridad - Disponibilidad	CONTINUIDAD OPERATIVA	2	Menor	2	Improbable	32	**BAJA**

Cuadro 32. (Continuación)

Ítem No.	Nombre del Activo	Proceso / Grupo	Tipo de Activo de información	Cargo Responsable	Custodio	Medio de almacenamiento	Ubicación	Estado del Activo	Propiedades de seguridad del activo de información						Valor del activo		Identificación vulnerabilidad y amenaza (causa)	Identificación del riesgo	Tipo de riesgo	Dueño del riesgo	Riesgo asociado a c-i-d	Tipo de impacto	Valor impacto	Nivel impacto	Valor probabilidad	Nivel probabilidad del riesgo	Valor riesgo	Nivel de riesgo
									Confidencialidad		Integridad		Disponibilidad															
									Nivel	Valor	Nivel	Valor	Nivel	Valor	Nivel	Valor												
37	Información sobre desplazamientos comisiones, tiquetes y viáticos	Gestión Financiera	Información Pura	Gerente Administrativo	Oficina Financiera	Combinado	Subdirección Financiera	Activo	Alta	4	Muy Alta	5	Muy Alta	5	Muy Alto	14	La Información sobre desplazamientos comisiones, tiquetes y viáticos, se procesa de forma manual. No se cuenta con una Sistema de información confiable, lo cual puede ocasionar errores.	Pérdida de disponibilidad de la información	Físico	Director Financiero	Integridad	CONTINUIDAD OPERATIVA	1	Insignificante	3	Moderada	42	BAJA
38	Documentos Word (minutas de contratos)	Gestión de Información	Información Pura	Secretario General de la Empresa	Secretario General de la Empresa	Combinado	Oficina Administrativa	Activo	Media	3	Media	3	Media	3	Medio	9	El almacenamiento del archivo en formato editable, además de un almacenamiento compartido, hace la información susceptible a ser modificada	Pérdida de la integridad de la información	Lógico	Secretario General	Integridad	LEGAL	2	Menor	2	Improbable	36	BAJA
39	información del Correo Electrónico	Gestión de Información	Información Pura	Jefe de Sistemas	Grupo Soporte Informático	Digital	Oficina de Sistemas - Soporte Informático	Activo	Media	3	Media	3	Baja	2	Medio	8	El funcionario realiza su propio Backup en un dispositivo extraíble (Disco Duro), la pérdida accidental de dicho dispositivo, puede ocasionar fuga de información.	Fuga de Información	Lógico	Gerente Administrativo	Confidencialidad	IMAGEN	2	Menor	2	Improbable	32	BAJA
40	Carpeta compartida Consecutivos	Gestión Financiera	Información Pura	Ejecutivo de Cuenta	Grupo Soporte Informático	Digital	Oficina de Sistemas - Soporte Informático	Activo	Media	3	Media	3	Baja	2	Medio	8	No se cuenta con permisos definidos para administrar la carpeta, la cual contiene información relevante para la ejecución de actividades en el área, sin embargo, el contenido puede ser modificado o borrado sin ningún control.	Pérdida de integridad y disponibilidad de la información	Lógico	Gerente Administrativo	Confidencialidad - Integridad - Disponibilidad	CONTINUIDAD OPERATIVA	2	Menor	3	Moderada	48	BAJA
41	Información de procesos y procedimientos en proceso de publicación.	Gestión de Información	Información Pura	Ejecutivo de Cuenta	Ejecutivo de Cuenta	Digital	Oficina Operativa	Activo	Media	3	Media	3	Muy Alta	5	Alto	11	El funcionario realiza su propio Backup en un dispositivo extraíble (Disco Duro), la pérdida accidental de dicho dispositivo, puede ocasionar fuga de información	Pérdida de la disponibilidad de la información	Lógico	Gerente Administrativo	Confidencialidad	IMAGEN	2	Menor	2	Improbable	44	BAJA
42	Información de procesos y procedimientos en proceso de publicación.	Gestión de Información	Información Pura	Ejecutivo de Cuenta	Ejecutivo de Cuenta	Digital	Oficina Operativa	Activo	Media	3	Media	3	Muy Alta	5	Alto	11	Por desconocimiento de las leyes vigentes y las políticas de seguridad de la información, los funcionarios o proveedores podrían divulgar información confidencial de Acceso Directo Asociados Limitada o personal de los usuarios.	Pérdida de Confidencialidad de la Información	Lógico	Gerente Administrativo	Disponibilidad	CONTINUIDAD OPERATIVA	2	Menor	2	Improbable	32	BAJA

Fuente: autores

6.4.5 Identificación de riesgo. Se identifican los eventos relevantes que pueden impactar de alguna forma el cumplimiento de los requisitos de seguridad de la información, debe tenerse en cuenta en este proceso la causa de origen del riesgo y el proceso o actividad que puede llegar a afectar**.**

Los riesgos identificados con base al inventario de activos son los siguientes:

- Pérdida de la integridad y disponibilidad de la información.
- Pérdida de la confidencialidad, integridad y/o disponibilidad de la información.
- Pérdida de la integridad y disponibilidad de la información.
- Pérdida de la autenticación de origen de la información.
- Pérdida de la integridad de la información.
- Pérdida de disponibilidad de la información.
- Pérdida de la confidencialidad de la información.
- Pérdida de la integridad de la información.
- Pérdida de la trazabilidad de la información.
- Pérdida de la integridad y disponibilidad de la información.
- Pérdida de imputabilidad.
- Fuga de Información.
- Reprocesos.
- Pérdida de Confidencialidad de la Información.
- Incumplimiento legal.

6.5 CONTROLES Y PLANES DE TRATAMIENTO

A continuación, se enuncian los controles y planes de tratamiento.

6.5.1 Plan de tratamiento de riesgos. Los planes de tratamiento de riesgos salen después de haber realizado una agrupación de los mismos, es decir, se identifican cuales riesgos tienen amenazas y/o vulnerabilidades en común y pueden ser tratados mediante los mismos controles, partiendo del hecho de que un control puede servir para más de un riesgo en la mayoría de los casos.

A continuación, en el Cuadro 33. Controles y tratamiento de riesgos se describen los pasos a seguir para el tratamiento a los riesgos identificados.

Cuadro 33. Controles y tratamiento de riesgos

N°	Riesgos encontrados	Activo Relacionado	Causa	Tratamiento	Control	Actividad	Referencia Anexo A ISO 27001:2013	Responsable	Recursos adicionales	Fecha de Inicio	Fecha de Fin	Observaciones
1	Deterioro de la Reputación	Base de datos de seguimiento de los procesos disciplinarios	La información que se almacena en las bases de datos es reportada por todos los clientes y proveedores del territorio colombiano, Acceso Directo, puede tomar decisiones administrativas equivocadas en caso que dicha información no sea integra y veraz.	Compartir el riesgo	Control 1	Implementar procesos legales para asegurar que la información entregada sea integra; se debe incluir firma de cláusulas y acuerdos.	A.15 A.15.1.1	Gerente Administrativo	N. A	Prioritario	Prioritario	N. A
		Información de la base de datos de Clientes										
		Información de la base de datos de registro y seguimiento de servicios	La información que se almacena en las bases de datos y que es reportada a Acceso Directo Asociados Limitada corresponde a la actualización del mes inmediatamente anterior. Por lo tanto, Acceso Directo, podría tomar decisiones administrativas equivocadas o tardías en caso de un evento inesperado que requiera acciones inmediatas por parte de Acceso Directo.	Mitigar el riesgo	Control 2	Involucrar un proceso de relacionamiento para la gestión del servicio entre el Acceso Directo, los clientes y proveedores que contemplen: * Hacer seguimiento de los niveles de desempeño de servicio para verificar el cumplimiento de los acuerdos; * Revisar los reportes de servicio elaborados por los clientes * llevar a cabo auditorías, junto con la revisión de reportes de auditores independientes, si están disponibles, y acciones sobre las cuestiones identificadas; * Revisar los rastros de auditoría del proveedor, y los registros de eventos de seguridad de la información, problemas operacionales, fallas, rastreo de fallas e interrupciones relacionadas con los reportes entregados *Resolver y gestionar cualquier problema identificado.	A.15.2.1 A.15.2.2	Jefe de Sistemas	N. A	Prioritario	Prioritario	N. A
		Información de la base de datos de contratos (Excel)										
		Información de la base de datos de Procesos (Excel)										

Cuadro 33. (Continuación)

N°	Riesgos encontrados	Activo Relacionado	Causa	Tratamiento	Control	Actividad	Referencia Anexo A ISO 27001:2013	Responsable	Recursos adicionales	Fecha de Inicio	Fecha de Fin	Observaciones
2	Fuga de Información	Información Contractual, estudios previos, informes, análisis licitaciones del Estado.	En las estaciones de trabajo no existen controles de seguridad para la fuga de información por medio de dispositivos ópticos como (CD) Y dispositivos extraíbles como (Discos duros, memorias USB).	Mitigar el riesgo	Control 3	* implementar el procedimiento para la gestión de medios removibles, el cual debe contemplar los siguientes aspectos a) Si ya no se requiere, el contenido de cualquier medio reusable que se vaya a retirar de la organización se debería remover de forma que no sea recuperable; b) Cuando resulte necesario y práctico, se debería solicitar autorización para retirar los medios de la organización, y se debería llevar un registro de dichos retiros con el fin de mantener un rastro de auditoría; c) Todos los medios se deberían almacenar en un ambiente protegido y seguro, de acuerdo con las especificaciones de los fabricantes; d) Si la confidencialidad o integridad de los datos se consideran importantes, se deberían usar técnicas criptográficas para proteger los datos que se encuentran en los medios removibles; e) Para mitigar el riesgo de degradación de los medios mientras aún se necesitan los datos almacenados, los datos se deberían transferir a medios nuevos antes de que se vuelvan ilegibles; f) Se deberían guardar varias copias de los datos valiosos en medios separados, para reducir aún más el riesgo de daño o pérdida casuales de los datos; g) Se debería considerar el registro de los medios removibles para reducir la oportunidad de pérdida de datos; h) Sólo se deberían habilitar unidades de medios removibles si hay una razón de negocio para hacerlo; i) En donde hay necesidad de usar medios removibles, se deberá hacer seguimiento a la transferencia de información a estos medios	A.10.7.1 A.10.7.2	Jefe de Sistemas	N. A	Prioritario	Prioritario	N. A

Cuadro 33. (Continuación)

N°	Riesgos encontrados	Activo Relacionado	Causa	Tratamiento	Control	Actividad	Referencia Anexo A ISO 27001:2013	Responsable	Recursos adicionales	Fecha de Inicio	Fecha de Fin	Observaciones
3	Pérdida de imputabilidad	Sistema maestro de vigilancia CCTV.	Las cámaras analógicas no cuentan con una buena resolución y en ocasiones no se reconoce a la persona grabada.	Mitigar el riesgo	Control 4	* En los próximos contratos de prestación de servicios de vigilancia, se debe incluir los requisitos de resolución de las cámaras de grabación, para el caso de las cámaras propias de Acceso Directo Asociados Limitada: Definir el nivel de resolución mínima que garantice la integridad de la información en una grabación Identificar las cámaras que cumplen con el requisito anterior, Buscar la realización de uno o varios contratos de renovación de las cámaras de vigilancia, teniendo en cuenta el presupuesto y el tiempo de implementación.	A.11.1.1 A.11.1.2	Gerente Administrativo	N. A	Prioritario	Prioritario	N. A
		Informe de depuración de datos. Información del Correo Electrónico	No existen políticas que definan el buen uso de los sistemas de información que se manejan en Acceso Directo Limitada, un funcionario o contratista accidental o deliberadamente puede hacer mal uso de los mismos, sin que haya consecuencias.	Mitigar el riesgo	Control 5	Cuando se aprueben y divulguen las políticas de seguridad de la información de Acceso Directo, estas deben ser aceptadas por todos los funcionarios, contratistas y proveedores de la empresa, mediante una firma escrita; lo anterior asegura el derecho de Acceso Directo al principio de repetición y a la investigación sin restricciones de un delito informático. Para ellos previamente, el acceso directo debe aprobar, difundir y sensibilizar a los funcionarios, contratistas y proveedores todas las políticas de seguridad de la información. Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.	A.5.1 A.5.1.1 A.7.2.2	Jefe de Sistemas	N. A	Prioritario	Prioritario	N. A
4	Pérdida de integridad de la información	Información de novedad del personal (incapacidad, vacaciones, licencias, certificaciones retención en la fuente, resoluciones de encargo, prima técnica, solicitudes de embargos)	Personas no autorizadas puede consultar y modificar documentos de novedad del personal todas las áreas.	Mitigar el riesgo	Control 6	*Revisar los derechos de acceso de a los activos de información de los usuarios; *Asignar los derechos de acceso a usuarios con base en la necesidad de uso y caso por caso, *Mantener un proceso de autorización y un registro de todos los privilegios asignados. Sólo se deberían suministrar derechos de acceso cuando el proceso de autorización esté completo; *Aplicar el principio del menor privilegio.	A.6.1.2 A.14.1.3 A.9.2.4 A.9.2.5	Gerente Administrativo	N. A	Prioritario	Prioritario	N. A

Cuadro 33. (Continuación)

N°	Riesgos encontrados	Activo Relacionado	Causa	Tratamiento	Control	Actividad	Referencia Anexo A ISO 27001:2013	Responsable	Recursos adicionales	Fecha de Inicio	Fecha de Fin	Observaciones
5	Pérdida de la confidencialidad de la información	Carpetas Compartidas (Registro de información General)	En las estaciones de trabajo no existen controles de seguridad para la fuga de información por medio de dispositivos ópticos como (CD) Y dispositivos extraíbles como (Discos duros, memorias USB).	Mitigar el riesgo	Control 7	* implementar el procedimiento para la gestión de medios removibles, el cual debe contemplar los siguientes aspectos a) Si ya no se requiere, el contenido de cualquier medio reusable que se vaya a retirar de la organización se debería remover de forma que no sea recuperable; b) Cuando resulte necesario y práctico, se debería solicitar autorización para retirar los medios de la organización, y se debería llevar un registro de dichos retiros con el fin de mantener un rastro de auditoría; c) Todos los medios se deberían almacenar en un ambiente protegido y seguro, de acuerdo con las especificaciones de los fabricantes; d) Si la confidencialidad o integridad de los datos se consideran importantes, se deberían usar técnicas criptográficas para proteger los datos que se encuentran en los medios removibles; e) Para mitigar el riesgo de degradación de los medios mientras aún se necesitan los datos almacenados, los datos se deberían transferir a medios nuevos antes de que se vuelvan ilegibles; f) Se deberían guardar varias copias de los datos valiosos en medios separados, para reducir aún más el riesgo de daño o pérdida casuales de los datos; g) Se debería considerar el registro de los medios removibles para reducir la oportunidad de pérdida de datos; h) Sólo se deberían habilitar unidades de medios removibles si hay una razón de negocio para hacerlo; i) En donde hay necesidad de usar medios removibles, se deberá hacer seguimiento a la transferencia de información a estos medios	A.8.3.1 A.8.3.2	Jefe de Sistemas	N. A	Prioritario	Prioritario	N. A
		Información Contractual y técnica de las licitaciones con el Estado.	El desconocimiento del procedimiento para la entrega formal de solicitudes de información para los proveedores, puede ocasionar que entre los funcionarios o contratistas se comparta información confidencial	Mitigar el riesgo	Control 8	* implementar programas de sensibilización y divulgación de las políticas de seguridad de la información. *Realizar la gestión de incidentes adecuada y aplicar las lecciones aprendidas. * Verificar y aplicar los acuerdos de confidencialidad de los contratos.	A.7.2.2	Jefe de Sistemas	N. A	Prioritario	Prioritario	N. A
		Documento de seguridad y salud en el trabajo	Este archivo presenta un alto grado de confidencialidad por lo que se requiere exclusividad de almacenamiento.	Mitigar el riesgo	Control 9	* Buscar alternativas para separar la información confidencial de la de trabajo diario, realizando una adecuada gestión de llaves y separación de privilegios, así mismo aplicar el procedimiento de etiquetado de la información.	A.8.2.2 A.9.2 A.11.1	Director Gestión del Talento Humano	N. A	Prioritario	Prioritario	N. A

Cuadro 33. (Continuación)

N°	Riesgos encontrados	Activo Relacionado	Causa	Tratamiento	Control	Actividad	Referencia Anexo A ISO 27001:2013	Responsable	Recursos adicionales	Fecha de Inicio	Fecha de Fin	Observaciones
6	Pérdida de la confidencialidad, integridad y disponibilidad de la información	Documentos de todas las dependencias	El acceso al archivo y a la oficina del grupo no es restringido, personal no autorizado puede ingresar a la oficina	Mitigar el riesgo	Control 10	Buscar controles adicionales para identificar posibles intrusos en las oficinas de procesamiento o almacenamiento de información; para esto se debe: a) Definir los perímetros de seguridad. La fortaleza de cada uno de los perímetros depende de los requisitos de seguridad de los activos dentro del perímetro y de los resultados de una valoración de riesgos; b) En donde sea aplicable, se deberían construir barreras físicas para impedir el acceso físico no autorizado y la contaminación ambiental; c) Todas las puertas contra incendio en un perímetro de seguridad deberían tener alarmas, estar monitoreadas y probadas junto con las paredes, para establecer el nivel requerido de resistencia de acuerdo con normas regionales, nacionales e internacionales	A.11.1 A.11.1.2	Director Gestión del Talento Humano	N. A	Prioritario	Prioritario	N. A
		Información de los expedientes de los procesos disciplinarios						Jefe de Sistemas	N. A	Prioritario	Prioritario	N. A
		Carpeta compartida Consecutivos (Orden de Servicio- Cotizaciones)						Ejecutivo de Cuenta	N. A	Prioritario	Prioritario	N. A
		SGA (Sistema de Información de Acceso Directo)	El archivo físico no está en un área segura, es vulnerable a daños físicos de las carpetas y a la pérdida de información, aunque está en proceso digitalización aún falta un escáner especial para su proceso	Mitigar el riesgo	Control 11	* Aplicar las directrices dadas por el Archivo General de la Nación	A.11.1.4	Gerente Administrativo	N. A	Prioritario	Prioritario	N. A
		SERVIDOR CORREO ELECTRÓNICO						Jefe de Sistemas	N. A	Prioritario	Prioritario	N. A
		SERVIDOR DE IMPRESIÓN	Dado que no cuentan con la definición de roles de usuarios. Lo anterior, implica que todos los funcionarios cuenten con privilegios adicionales a los que realmente necesitan para el normal desempeño de sus funciones.	Mitigar el riesgo	Control 12	Crear Roles de Usuarios. Los administradores de sistemas no deberían tener permiso para borrar o desactivar logs de sus propias actividades.	A.12.4.1 A.12.4.2 A.12.4.3 A.12.4.4 A.16.1.7 A.18.1.4	Jefe de Sistemas	N. A	Prioritario	Prioritario	N. A
		SERVIDOR DE TELEFONÍA										
		Estaciones de Trabajo del Acceso Directo Asociados Limitada	No se conoce el procedimiento de los niveles de acceso a las aplicaciones y servidores del Acceso Directo Asociados Limitada, por esta razón se le puede dar acceso a cualquier persona que lo solicite sin ser autorizado.	Evitar el riesgo	Control 13	* Se debe implementar y documentar un procedimiento de autorización de acceso a usuarios, los accesos deben ser solicitados o autorizados por el jefe o propietario de cada proceso. Este procedimiento debe contar con el apoyo de Gestión del Talento Humano.	A.9.2.2	Jefe de Sistemas	N. A	Prioritario	Prioritario	N. A
		Carpetas Historias Laborales	En las estaciones de trabajo no existen controles de seguridad para la fuga de información por medio de dispositivos ópticos como (CD) Y dispositivos extraíbles como (Discos duros, memorias USB).	Asumir el riesgo	Control 14	* A futuro se debe incluir la gestión de medios removibles a través de consolas de antivirus las cuales permiten el registro de dispositivos removibles, seguimiento mediante logs y gestión de llaves. Incluir la adquisición y gestión de sistemas DLP (data Loss Prevention)	A.8.3.1	Director Gestión del Talento Humano	N. A	Prioritario	Prioritario	N. A
		UPS centro de cómputo (Backup 30 KVA)						Jefe de Grupo de Soporte informático	N. A	Prioritario	Prioritario	N. A

Cuadro 33. (Continuación)

N°	Riesgos encontrados	Activo Relacionado	Causa	Tratamiento	Control	Actividad	Referencia Anexo A ISO 27001:2013	Responsable	Recursos adicionales	Fecha de Inicio	Fecha de Fin	Observaciones
7	Pérdida de la continuidad del proceso	Plan de acción y Plan de adquisidores	La disposición física de las carpetas físicas, así como el uso y traslados necesarios para la ejecución de las labores, expone la información ante personas no autorizadas para tener conocimiento sobre el mismo o a condiciones ambientales o humanas que lleven a una eventual pérdida de la información.	Asumir el riesgo	Control 15	* Generar campañas de sensibilización sobre el uso y traslado de información que se genere en la empresa compromiso y responsabilidad sobre la información que maneja. * Definir e implementar un procedimiento de etiquetado y clasificación de la información que ayude al control e identificación de la información tanto en su generación, transito o destrucción. * Incluir archivos que permitan el almacenamiento seguro de la información implementando controles que permitan la trazabilidad del uso o préstamo de la información.	A.8.2.2 A.8.3.3	Gerente Administrativo	N. A	Prioritario	Prioritario	N. A
8	Pérdida de la disponibilidad de la información	Historias clínicas Bodega de Datos	Este archivo presenta un alto grado de confidencialidad por lo que se requiere exclusividad de almacenamiento,	Mitigar el riesgo	Control 16	* Definir políticas de control de acceso a la información y a los sistemas de información. *Definir políticas de almacenamiento de información tanto física como en los sistemas de información definiendo las responsabilidades. Debe ir alineado con el procedimiento de Clasificación y Etiquetado de la Información de Acceso Directo. * Realizar revisiones periódicas de los derechos de acceso por parte de los usuarios a la información y a los sistemas de información de Acceso Directo.	A.8.2.1 A.8.2.2 A.8.2.3 A.9.1.1 A.9.2.3 A.9.4.1 A.9.4.2	Jefe de Sistemas	N. A	Prioritario	Prioritario	N. A
		Expedientes de contratación (están en físico)	No se mantiene un registro de a quién se le prestan los expedientes, la manipulación y tiempo que permanecen éstas sin almacenar combinado con la falta de cámaras de seguridad y aislamiento del área, puede implicar traslados no deseados o pérdida de la información	Compartir el riesgo	Control 17	* Establecer políticas de manejo de los activos de información en donde se considere los roles responsables. Cuando los activos son retirados, debe quedar registro documentado y aprobación del propietario del mismo. * Implementar controles de seguridad como cámaras de vigilancia que permitan el monitoreo y control de las instalaciones. * Definir los perímetros de seguridad y el control de acceso a las instalaciones.	A.8.2.3 A.11.1.1 A.11.1.2	Jefe Gestión del Talento Humano	N. A	Prioritario	Prioritario	N. A
		Archivo físico (expedientes y archivos de gestión)	Las cámaras de baja definición o ausencia de las mismas disminuyen el control efectivo sobre la documentación.	Mitigar el riesgo	Control 18	* Implementar controles de seguridad como cámaras de vigilancia que permitan el monitoreo y control de las instalaciones. * Definir los perímetros de seguridad y el control de acceso a las instalaciones.	A.11.1.1 A.11.1.2	Gerente Administrativo	N. A	Prioritario	Prioritario	N. A

Cuadro 33. (Continuación)

N°	Riesgos encontrados	Activo Relacionado	Causa	Tratamiento	Control	Actividad	Referencia Anexo A ISO 27001:2013	Responsable	Recursos adicionales	Fecha de Inicio	Fecha de Fin	Observaciones
9	Pérdida de la integridad de la información	Base de Datos de contratos (Excel)	El almacenamiento del archivo en formato editable, además de un almacenamiento compartido, hace la información susceptible a ser modificada	Mitigar el riesgo	Control 19	* Establecer un procedimiento de firma digital en la documentación critica el cual garantice la integridad de la información.	A.10.1.1 A.10.1.2	Director Gestión del Talento Humano	N. A	Prioritario	Prioritario	N. A
		Archivos de pago de nómina/terceros/ entidades financieras	Los archivos de pago de nómina, a terceros o entidades financieras, se consolidan mediante un proceso manual (En Excel). Una persona podría cambiar accidental o intencionalmente el valor del pago que se debe realizar en el Acceso Directo Asociados Limitada.	Mitigar el riesgo	Control 20	* Realizar sensibilizaciones y toma de conciencia a los funcionarios de Acceso Directo Asociados Limitada sobre la seguridad de la información. * Establecer un procedimiento de firma digital en la documentación critica el cual garantice la integridad de la información.	A.7.2.2 A.10.1.1 A.10.1.2	Secretario General	N. A	Prioritario	Prioritario	N. A
		Cintas magnéticas.	Los Backups, se almacenan en cintas guardadas en cajas sin ningún control de seguridad, los cuales son vulnerables a la humedad y daños físicos, afectando la integridad de la información.	Mitigar el riesgo	Control 21	* Definir un procedimiento de Copias de Respaldo (Backups) en donde se especifiquen los sistemas críticos de información a respaldar, la periodicidad, los responsables, el almacenamiento seguro de los medios (cintas, discos) y el método de realizar la restauración cuando sea necesario.	A.12.3.1	Jefe de Sistemas	N. A	Prioritario	Prioritario	N. A

Cuadro 33. (Continuación)

N°	Riesgos encontrados	Activo Relacionado	Causa	Tratamiento	Control	Actividad	Referencia Anexo A ISO 27001:2013	Responsable	Recursos adicionales	Fecha de Inicio	Fecha de Fin	Observaciones
10	Pérdida de la integridad y disponibilidad de la información	Carpeta compartida Comercial (Procesos de Licitaciones, cámara de comercio, RUT, RUP, RITk, Cedulas de Representantes legales)	No se cuenta con permisos definidos para administrar la carpeta compartida, la cual contiene información relevante para la ejecución diaria e actividades en el área, sin embargo, el contenido de la carpeta puede ser modificado o borrado sin ningún control.	Mitigar el riesgo	Control 22	* Documentar, implementar y difundir políticas de control de acceso de usuarios a la información y a los sistemas de información. * Establecer un procedimiento de registro, monitoreo y cancelación de acceso de usuarios a los sistemas de información. * Realizar revisión periódica de los controles de acceso establecidos para la información y los sistemas de información de Acceso Directo. * Restringir el acceso a información confidencial y garantizar solo el acceso por personal autorizado. * Establecer un procedimiento de Gestión de Contraseñas para Acceso Directo Asociados Limitada y asegurar que todos los sistemas de información y almacenamiento cuenten con un control de ingreso.	A.9.1.1 A.9.1.2 A.9.2.1 A.9.2.2 A.9.2.3 A.9.2.4 A.9.2.5 A.9.2.6	Ejecutivo de Cuenta	N. A	Prioritario	Prioritario	N. A
		Documentos de novedad del personal (incapacidad, vacaciones, horas extras, licencias, solicitudes de descuentos para sindicatos, certificaciones retención en la fuente, resoluciones de encargo, prima técnica, solicitudes de embargos)	Documentos de novedad del personal se almacenan en una carpeta compartida sin permisos definidos. Una persona podría cambiar o borrar accidental o intencionalmente el contenido de dicha carpeta	Mitigar el riesgo	Control 23	* Documentar, implementar y difundir políticas de control de acceso de usuarios a la información y a los sistemas de información. * Establecer un procedimiento de registro, monitoreo y cancelación de acceso de usuarios a los sistemas de información. * Realizar revisión periódica de los controles de acceso establecidos para la información y los sistemas de información de Acceso Directo. * Restringir el acceso a información confidencial y garantizar solo el acceso por personal autorizado. * Establecer un procedimiento de Gestión de Contraseñas para y asegurar que todos los sistemas de información y almacenamiento cuenten con un control de ingreso.	A.9.1.1 A.9.1.2 A.9.2.1 A.9.2.2 A.9.2.3 A.9.2.4 A.9.2.5 A.9.2.6	Secretario General/ Jefe de Sistemas	N. A	Prioritario	Prioritario	N. A
11	Reprocesos	Equipo cómputo del Ejecutivo de Cuenta	El almacenamiento de información en una estación de trabajo de uso operativo constante, sin una copia de respaldo adecuada, lo cual puede ocasionar pérdidas de información a causa de fallas en hardware o software en el equipo	Mitigar el riesgo	Control 24	* Definir un procedimiento de Copias de Respaldo (Backups) en donde se especifiquen los sistemas críticos de información a respaldar, la periodicidad, los responsables, el almacenamiento seguro de los medios (cintas, discos) y el método de realizar la restauración cuando sea necesario.	A.12.3.1	Jefe de Sistemas	N. A	Prioritario	Prioritario	N. A

Fuente: Autores

En el Cuadro 33. Controles y tratamiento de riesgos, se agrupan los riesgos encontrados en 11 riesgos de importancia relevante para los activos de información de la empresa Acceso Directo Asociados Limitada, los cuales pueden ser mitigados, compartidos, eliminados o aceptados en 24 controles que dan como resultado del estudio de los riesgos y los controles sugeridos por la norma ISO 27001:2013, la aplicación de estos 24 controles garantizan la protección adecuada de los objetivos e ideales de negocio de la empresa Acceso Directo Asociados Limitada, puesto que estos están directamente ligados a los activos de información de la misma.

6.6 POLÍTICAS

A continuación, se expondrán las políticas que se aplican a la empresa.

6.6.1 Política general. En Acceso Directo Asociados Limitada la información es un activo primordial para la prestación de sus servicios y la toma de decisiones eficientemente, razón por la cual debe haber un compromiso claro de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y el afianzamiento de una cultura de seguridad.

Consiente de las necesidades actuales, Acceso Directo Asociados Limitada con un modelo de gestión de seguridad de la información; como herramienta que permite identificar y reducir los riesgos a los cuales se expone la información, beneficia a la disminución de costos operativos y financieros, construye una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

Los funcionarios, proveedores y todos aquellos que tengan responsabilidades sobre los recursos de procesamiento de la información de Acceso Directo Asociados Limitada, deben adoptar los lineamientos contenidos en el documento de las políticas, con el propósito de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

La política general de seguridad de la Información de Acceso Directo Asociados Limitada se encuentra soportada por políticas, normas y procedimientos específicos los cuales guiarán el manejo adecuado de la información de la empresa. Adicionalmente, se establecerán políticas específicas de seguridad de la información las cuales se establecen en los dominios y objetivos de control del Anexo A de la norma internacional ISO 27001:2013.

La gerencia tendrá la autoridad de modificar la política general o las políticas específicas de seguridad de la información de acuerdo con las necesidades de revisión establecidas periódicamente o a la aplicabilidad de las mismas.

Objetivo: Ofrecer apoyo y orientación a la gerencia de Acceso Directo Asociados Limitada con relación a la seguridad de la información, de acuerdo con los requisitos del negocio y los controles asociados al plan de tratamiento de riesgos.

Alcance: Las políticas de seguridad de la información se aplican a los aspectos administrativos y de control que deben ser cumplidos por la gerencia, empleados, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con Acceso Directo Asociados Limitada, para el debido cumplimiento de sus funciones y para lograr un apropiado nivel de protección en la seguridad de la información, aportando con su participación en la toma de medidas preventivas y correctivas. El personal de Acceso Directo Asociados Limitada tiene el compromiso de dar cumplimiento a las políticas emitidas y aprobadas por la gerencia.

6.6.2 Políticas específicas de seguridad de la información. A continuación, se enuncian las políticas de seguridad de la información.

6.6.2.1 Política de seguridad de la información (A.5). La Gerencia de Acceso Directo Asociados Limitada será la responsable de la aprobación y divulgación de las políticas de seguridad de la información, estas deben ser aceptadas por todos los funcionarios, contratistas y proveedores de la empresa, mediante una firma escrita; lo anterior asegura el derecho de Acceso Directo Asociados Limitada al principio de repetición y a la investigación sin restricciones de un delito informático. Para ello previamente, la empresa Acceso Directo Asociados Limitada debe aprobar, difundir y sensibilizar a los funcionarios, contratistas y proveedores todas las políticas de seguridad de la información.

Las políticas para seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúa.

6.6.2.2 Organización de la seguridad de la información (A.6). La responsabilidad de la seguridad de la información, no es competencia únicamente de la gerencia de Acceso Directo Asociados Limitada, es una obligación de todas

las áreas que componen la empresa y de cada uno de los funcionarios de la misma.

El personal de Acceso Directo Asociados Limitada, no debe suministrar ningún tipo de información de la empresa a personas externas o internas sin las autorizaciones respectivas.

La oficina de sistemas de la empresa Acceso Directo Asociados Limitada, debe revisar los derechos de acceso de a los activos de información de los usuarios, de igual forma asignar los derechos de acceso a usuarios con base en la necesidad de uso y caso por caso.

Se debe mantener un proceso de autorización y un registro de todos los privilegios asignados. Sólo se deberían suministrar derechos de acceso cuando el proceso de autorización esté completo.

Se contempla en casos específicos aplicar el principio del menor privilegio.

6.6.2.3 Gestión de activos (A.7). Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, la gerencia de la empresa Acceso Directo Asociados Limitada, con la colaboración de la oficina de sistemas debe implementar programas de sensibilización y divulgación de las políticas de seguridad de la información.

Es responsabilidad de los funcionarios de la empresa realizar la gestión de incidentes adecuada y aplicar las lecciones aprendidas.

Los funcionarios de la empresa están en el deber de verificar y aplicar los acuerdos de confidencialidad de los contratos.

Se debe realizar sensibilizaciones y toma de conciencia a los funcionarios de Acceso Directo Asociados Limitada sobre la seguridad de la información.

6.6.2.4 Seguridad de los recursos Humanos (A.8)**.** El personal vinculado con la empresa Acceso Directo Asociados Limitada, debe conocer y poner en práctica la presente política independientemente del tipo de vinculación que tenga con la

empresa, todo el personal está en la obligación de mantener la confidencialidad de la información que le sea entregada para el desarrollo de sus actividades o información a la que tenga acceso de forma voluntaria o involuntaria.

Se deben establecer políticas de manejo de los activos de información en donde se considere los roles responsables. Cuando los activos son retirados, debe quedar registro documentado y aprobación del propietario del mismo.

La gerencia de la empresa Acceso Directo Asociados Limitada debe generar campañas de sensibilización sobre el uso y traslado de información que se genere en la empresa, el compromiso y responsabilidad sobre la información y el funcionario que la maneja.

Es responsabilidad de la oficina de sistema definir e implementar un procedimiento de etiquetado y clasificación de la información que ayude al control e identificación de la información tanto en su generación, transito o destrucción.

Es necesario incluir archivos que permitan el almacenamiento seguro de la información implementando controles que permitan la trazabilidad del uso o préstamo de la información.

6.6.2.5 Seguridad física y del entorno (A.9). La gerencia de la empresa Acceso Directo Asociados Limitada, debe implementar y documentar un procedimiento de autorización de acceso a usuarios, los accesos deben ser solicitados o autorizados por el jefe o propietario de cada proceso. Este procedimiento debe contar con el apoyo de Gestión del Talento Humano.

La gerencia de la empresa en coordinación con la oficina de sistemas es responsable de documentar, implementar y difundir políticas de control de acceso de usuarios a la información y a los sistemas de información.

Para todos los funcionarios de Acceso Directo Asociados Limitada, se debe establecer un procedimiento de registro, monitoreo y cancelación de acceso de usuarios a los sistemas de información.

Es responsabilidad de la gerencia o de quien está delegue realizar revisión periódica de los controles de acceso establecidos para la información y los sistemas de información de Acceso Directo Asociados Limitada.

La oficina de sistemas es responsable de restringir el acceso a información confidencial y garantizar solo el acceso por personal autorizado y establecer un procedimiento de gestión de contraseñas para Acceso Directo Asociados Limitada, y asegurar que todos los sistemas de información y almacenamiento cuenten con un control de ingreso.

6.6.2.6 Gestión de comunicaciones y operaciones (A.10). La oficina de sistemas debe implementar el procedimiento para la gestión de medios removibles, el cual debe contemplar los siguientes aspectos:

a) Si ya no se requiere, el contenido de cualquier medio reusable que se vaya a retirar de la organización se debería remover de forma que no sea recuperable.

b) Cuando resulte necesario y práctico, se debería solicitar autorización para retirar los medios de la organización, y se debería llevar un registro de dichos retiros con el fin de mantener un rastro de auditoría.

c) Todos los medios se deberían almacenar en un ambiente protegido y seguro, de acuerdo con las especificaciones de los fabricantes.

d) Si la confidencialidad o integridad de los datos se consideran importantes, se deberían usar técnicas criptográficas para proteger los datos que se encuentran en los medios removibles.

e) Para mitigar el riesgo de degradación de los medios mientras aún se necesitan los datos almacenados, los datos se deberían transferir a medios nuevos antes de que se vuelvan ilegibles.

f) Se deberían guardar varias copias de los datos valiosos en medios separados, para reducir aún más el riesgo de daño o pérdida casuales de los datos.

g) Se debería considerar el registro de los medios removibles para reducir la oportunidad de pérdida de datos.

h) Sólo se deberían habilitar unidades de medios removibles si hay una razón de negocio para hacerlo.

i) En donde hay necesidad de usar medios removibles, se deberá hacer seguimiento a la transferencia de información a estos medios.

6.6.2.7 Control de acceso (A.11). La gerencia de la empresa en coordinación con la oficina de sistemas de la empresa Acceso Directo Asociados Limitada serán los

responsables de implementar controles de seguridad como cámaras de vigilancia que permitan el monitoreo y control de las instalaciones.

Es responsabilidad de la gerencia definir los perímetros de seguridad y el control de acceso a las instalaciones.

De acuerdo a las responsabilidades de cada funcionario y las actividades de cada cargo se implementarán procedimientos para la activación o desactivación de acceso a redes o recursos compartidos y de internet.

Teniendo en cuenta la clasificación de la información se establecerá el procedimiento de respaldo de información y backups.

Implementar controles adicionales para identificar posibles intrusos en las oficinas de procesamiento o almacenamiento de información; para esto se debe:

a) Definir los perímetros de seguridad. La fortaleza de cada uno de los perímetros depende de los requisitos de seguridad de los activos dentro del perímetro y de los resultados de una valoración de riesgos.

b) En donde sea aplicable, se deberían construir barreras físicas para impedir el acceso físico no autorizado y la contaminación ambiental.

c) Todas las puertas contra incendio en un perímetro de seguridad deberían tener alarmas, estar monitoreadas y probadas junto con las paredes, para establecer el nivel requerido de resistencia de acuerdo con normas regionales, nacionales e internacionales.

6.6.2.8 Adquisición, desarrollo y mantenimiento de sistemas de información (A.12). La oficina de sistemas de la empresa Acceso Directo Asociados Limitada, tiene la responsabilidad de diseñar un cronograma de mantenimiento tanto del servidor como de medios de almacenamiento con el fin de preservar la información.

Es responsabilidad de la oficina de sistemas crear roles de usuarios.

Los administradores de sistemas no deberían tener permiso para borrar o desactivar logs de sus propias actividades.

Se debe definir un procedimiento de copias de respaldo (backups) en donde se especifiquen los sistemas críticos de información a respaldar, la periodicidad, los responsables, el almacenamiento seguro de los medios (cintas, discos) y el método de realizar la restauración cuando sea necesario.

6.6.2.9 Cumplimiento (A.15). La empresa Acceso Directo Asociados Limitada, debe implementar procesos legales para asegurar que la información entregada sea integra; se debe incluir firma de cláusulas y acuerdos.

El personal de la empresa Acceso Directo Asociados Limitada, se debe involucrar a el proceso de relacionamiento para la gestión del servicio entre el Acceso Directo Asociados Limitada, los clientes y proveedores que contemplen.

Se debe hacer seguimiento de los niveles de desempeño de servicio para verificar el cumplimiento de los acuerdos.

La gerencia o quien está delegue estará encargada de revisar los reportes de servicio elaborados por los clientes.

Periódicamente se debe llevar a cabo auditorías, junto con la revisión de reportes de auditores independientes, si están disponibles, y acciones sobre las cuestiones identificadas.

Revisar los rastros de auditoría del proveedor, y los registros de eventos de seguridad de la información, problemas operacionales, fallas, rastreo de fallas e interrupciones relacionadas con los reportes entregados y resolver y gestionar cualquier problema identificado.

7. RESULTADOS ESPERADOS

El diseño de SGSI entregado a la empresa Acceso Directo Asociados Limitada tiene como finalidad mejorar el nivel seguridad de la información, minimizando riesgos potenciales a los cuales esta pueda estar expuesta, uno de los más importantes es la fuga de información, en especial de datos o archivos identificados como críticos o confidenciales, esto con el fin de que el prestigio de la empresa no se vea manchado por algún incidente de seguridad informática, minimizando de esta forma, la explotación en el mercado de nuevas oportunidades de negocio con nuevos clientes potenciales.

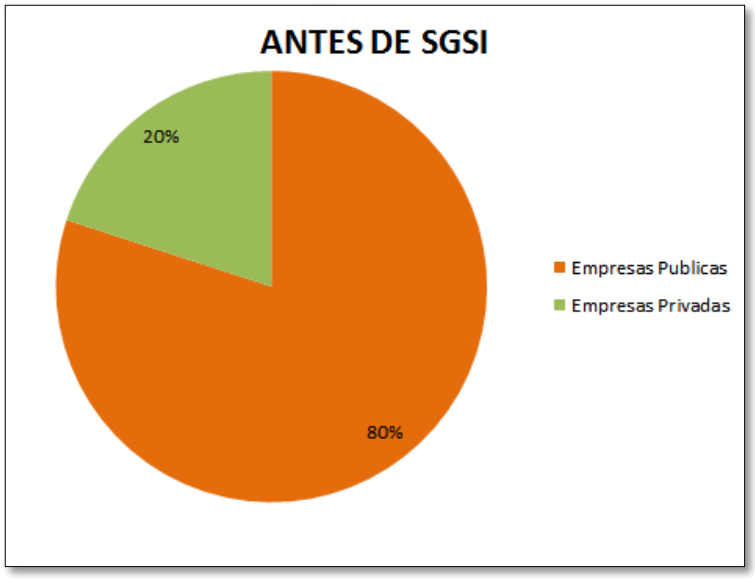
Con el Diseño del Sistema de Gestión de la Seguridad de la Información (SGSI) para la empresa Acceso Directo Asociados Limitada ayudará a establecer políticas y procedimientos en relación a la seguridad de la información, con el objetivo de preservar un nivel de exposición siempre menor al nivel de riesgo que la propia empresa decida asumir, esto con el fin de proteger de forma adecuada sus objetivos e ideales de negocio para así tener una mayor explotación de nuevas oportunidades en el mercado actual.

Nuevas oportunidades de negocio: Como se había descrito anteriormente en el documento, la empresa Acceso Directo Asociados Limitada tiene como base estratégica de mercado las empresas estatales, mediante licitaciones públicas, esto a razón de que los requisitos para contratar con entidades públicas son en su mayoría netamente contractuales y jurídicos, el diseño del gestión de seguridad de la información define pautas de protección de los activos de información de la empresa, lo que garantiza que la empresa Acceso Directo Asociados Limitada, está en condiciones de ingresar al mercado de la contratación directa con entidades privadas, ya que es un mercado poco explorado por la empresa, puesto que las exigencias de las entidades privadas en cuanto a la reserva, confidencialidad, integridad y disponibilidad de sus campañas publicitarias es mucho más alta y estricta.

En casos específicos que por acuerdos de confidencialidad no pueden ser mencionados la empresa Acceso Directo Asociados Limitada, ha perdido la posibilidad de concretar contratos directos con entidades privadas debido a sus bajos niveles de seguridad de la información, lo que genero desconfianza en los posibles clientes potenciales al existir la posibilidad de que su información se viera en manos de terceros no autorizados, el cuadro de controles y tratamientos determina controles precisos para asegurar la información de manera adecuada, al cumplir con este requisito se amplían las posibilidades de subir el 20% actual de contratos con empresas privadas a un 45%, datos que fueron tomados como

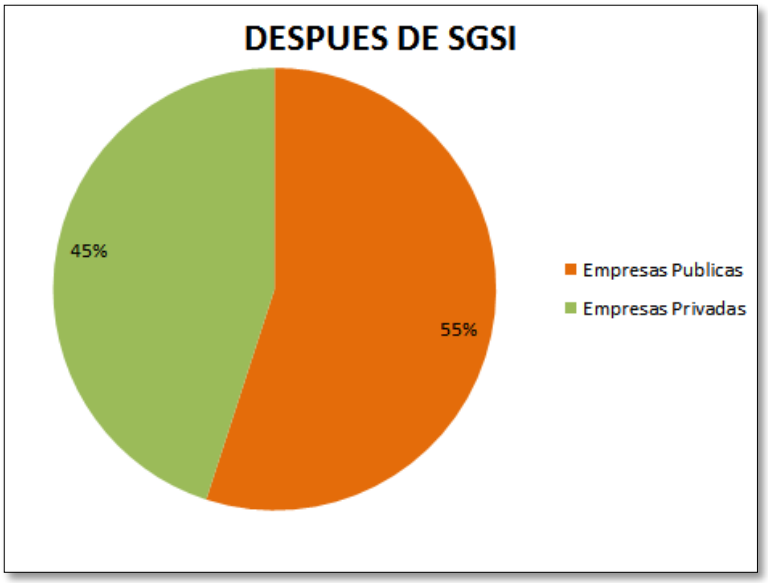
promedio de las ofertas perdidas por bajo nivel de protección de la información confidencial, reservada o crítica.

Gráfica 25. ANTES DE SGSI



Fuente: Autores.

Gráfica 26. DESPUÉS DEL SGSI



Fuente: Autores

8. CONCLUSIONES

El diseño de un sistema de gestión de seguridad de la información permitió a los autores del proyecto identificar los riesgos existentes en la empresa Acceso Directo Asociados Limitada, los cuales exponen los activos de información a algún tipo de vulnerabilidad o exposición a algún agente interno o externo que afecte su integridad, disponibilidad y confidencialidad; y realizar una clasificación de estos de acuerdo a valores dados a los riesgos, estableciendo así que los riesgos potencialmente peligrosos están clasificados como extremos, altos y moderados, los cuales deben ser analizados, evaluados y controlados hasta llevarlos a un nivel aceptable donde se vea una relación coherente costo-beneficio.

El establecimiento de una clasificación de activos proporcionó información relevante que permite afirmar que la clasificación de activos es independiente y muy diferente de una empresa a otra, ya que este tipo de clasificación se ajusta a las necesidades particulares de cada una, para Acceso Directo Asociados Limitada se platearon criterios de clasificación de acuerdo con las necesidades de la empresa y con el perfil del recurso humano que labora en ella.

La recolección de información de activos, análisis y evaluación de los mismos evidencia que la valoración de cada activo de información es determinada únicamente por el dueño del activo, el cual es el único que conoce el valor real que dicho activo representa para la empresa, en el análisis realizado en este proyecto se ve claramente que cada activo recibe una valoración distinta de acuerdo con los servicios prestados por el activo evaluado.

El diseño de un sistema de gestión de seguridad de la información y llegado al caso su implantación no es garantía de aseguramiento de los activos de información al 100%, sin embargo, si se garantiza que los riesgos reciban el adecuado tratamiento y sean llevados a un nivel aceptable o sea catalogado un riesgo inherente.

El análisis de riesgos realizado a los activos de información de la empresa Acceso Directo Asociados Limitada y su posterior tratamiento y definición del control asociado al mismo permitió a los autores del proyecto establecer las políticas de seguridad representativa y aplicable a la empresa Acceso Directo Asociados Limitada según los dominios de la norma ISO 27001:2013.

BIBLIOGRAFÍA

ACCESO DIRECTO. (28 de Noviembre de 2016). Obtenido de ACCESO DIRECTO: http://accesodirecto.com.co/web/es

ICONTEC. (2009). COMPENDIO SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). Bogotá: ICONTEC.

ISO 27000.es. (16 de Abril de 2016). Obtenido de ISO 27000: http://www.iso27000.es/sgsi.html

ISO 27001 2013: Pasos a seguir en una evaluación de riesgos. (19 de Febrero de 2017). Obtenido de SGSI Blog especializado en Sistemas de Gestión : http://www.pmg-ssi.com/2016/05/iso-27001-2013-pasos-seguir-evaluacion-riesgos/

Master en Gestión de Calidad y Reingenieria de Procesos. (s.f.). Obtenido de Master en Gestión de Calidad y Reingenieria de Procesos: http://www.eoi.es/blogs/mcalidadon/2016/02/03/la-matriz-probabilidad-impacto/

SGSI Blog especializado en Sistemas de Gestión . (16 de Abril de 2016). Obtenido de Blog especializado en Sistemas de Gestión : http://www.pmg-ssi.com/2015/07/que-es-sgsi/

SGSI Blog especializado en Sistemas de Gestión . (18 de Febrero de 2017). Obtenido de SGSI Blog especializado en Sistemas de Gestión : http://www.pmg-ssi.com/2015/05/como-clasificar-los-activos-de-seguridad-en-un-sgsi/

Sistema de Gestión de la Seguridad de la información. (3 de Marzo de 2017). Obtenido de Sistema de Gestión de la Seguridad de la información: http://www.iso27000.es/download/doc_sgsi_all.pdf

SISTEMA DE GESTIÓN DE SEGURIDAD LA INFORMACIÓN, ISO27001. (27 de Febrero de 2017). Obtenido de SISTEMA DE GESTIÓN DE SEGURIDAD LA INFORMACIÓN, ISO27001: http://www.ceeisec.com/nuevaweb/doc/FORMACION_SGSI_2010.pdf